Edwards Hall Primary School

Online Safety Policy

Reference:	Online Safety Policy
Responsibility of:	IT Co-ordinator
Date Issued:	May 2017
Governor Approved:	June 2017
Review Date:	June 2020

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Pupil and Curriculum Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body will take on the role of Online safety Governor, currently Mrs Faye Stone through her role of safe guarding responsibility.

Headteacher and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community**, though the day to day responsibility for online safety will be delegated to the Online safety Coordinator.
- **The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.** (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Incidents of cyber bullying will be reported in the as a bullying incident and logged with the Headteacher. Incidents of safe guarding around online safety will be logged with the Headteacher in the same way of an offline safe guarding incident.

Online safety Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff

Computing Coordinator/ Technical staff:

The Co-ordinator for Computing is responsible for ensuring:

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required online safety technical requirements and any Local Authority / other relevant body Online Safety Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password.**
- the filtering policy (for internet use provided by E2BN), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Principal / Senior Leader; Online safety Coordinator for investigation / action / sanction

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current school online safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy (AUP) which is in the appendix**
- **they report any suspected misuse or problem to the Headteacher) for investigation / action / sanction**
- **all digital communications with pupils / parents / carers should be on a professional level** and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- **in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches**

Designated Safeguarding Person

The DSP should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding 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:

- **are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- on-line student / pupil records supporting sites

Policy Statements

Education – pupils

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

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited. Where objectives are discrete, e-safety objectives can be covered on a continual basis whereas when discrete and link with other topics, they should be clearly highlighted in the computing coverage document.**
- **Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities as outlined at the end of the section.**
- **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**

- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- 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, staff should be vigilant in monitoring the content of the websites the young people visit.

Online Safety Events during the school year (although not limited to this)

Activity	**Key dates:**	**Time/cost resources:**	**Success criteria / Monitoring:**
1. New staff briefing on E-Safety at Edwards Hall.	Induction Period	Free	Staff aware of E-safety Policy and Acceptable Use Policy and are confident in delivering the content.
2. Separate Key Stage E-safety assembly on social media profiles and keeping information private.	September	Free	Children to share ideas on the child in the video could have stayed safe.
3. Support staff in ensuring E-safety coverage through planning – allow staff to identify opportunities for coverage – share ideas to help each other.	Throughout the year	Staff meeting	Staff planning shows coverage. Staff meeting agenda.
4. Y5 & 6 CEOP workshop – delivered by Anthony Peltier (Head @ Stifford Clays and in the Police Force)	Spring / Summer	Free	Children are aware of how to stay safe & how to raise alerts online. Photos & pupil voice.
5. Staff CEOP training – delivered by Anthony Peltier (Head @ Stifford Clays and in the Police Force)	Spring / Summer	Free (Staff meeting)	Staff are aware of CEOPs role, how to raise alerts
6. Parent CEOP training – delivered by Anthony Peltier (Head @ Stifford Clays and in the Police Force)	Spring / Summer	Free	Parents are aware of CEOPs role, acceptable usage & how to raise alerts. Parent feedback form
7. Whole School E-safety Assembly to introduce E-Safety day	February	Free	Children to share ideas on staying safe / how to solve an issue.
8. Participation in E-safety day https://www.saferinternetday.org/	February	Free	Children understand an aspect of E-safety in greater depth. Pupil Voice, Photos & work produced.
9. Separate Key Stage E-safety assembly keeping safe online with emphasis over summer holidays.	July	Free	Children to share ideas on the child in the video could have stayed safe.

Education – parents / carers

Many parents and carers have only a limited understanding of online 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

Education - Community

The school will provide opportunities for members of the community to gain from the school's online safety knowledge and experience. This is offered through the school website which provides online safety links.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A planned programme of formal online safety training is available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.**
- **All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.**
- The Online safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors take part in online safety training / awareness sessions.

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

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 online safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users** (from Year 1 and above) **will be provided with a username and secure password** by the computing technician. **Users are responsible for the security of their username and password** and will be required to change their password regularly.
- **The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)**
- **The Business manager, through the SLN, is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

<u>Mobile Technologies</u>

Mobile technology devices which are school owned including tablets, laptop or other technology that usually have the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The use of mobile technologies should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be a part of the school's Online Safety education programme. Students / Staff / Visitors should not be using personal mobile devices in school without prior permission.

<u>Use of digital and video images</u>

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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 eg on social networking sites.
- Permission should be obtained from parents or carers before photographs of the pupils are published in external sources such as the local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers will be obtained at the start of a pupil's school career as to whether photographs of pupils are allowed to be published on the school website.

<u>Data Protection</u>

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.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and pupils or parents / carers (email, text etc) must be professional in tone and content.** Personal email addresses, personal text messaging or social media must not be used for these communications.

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- School staff should ensure that:
- No negative references of the school should be made in social media to pupils, parents / carers or other school staff
- They do not engage in online discussion on personal matters relating to members of the school community which could bring themselves or the school into disrepute
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

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

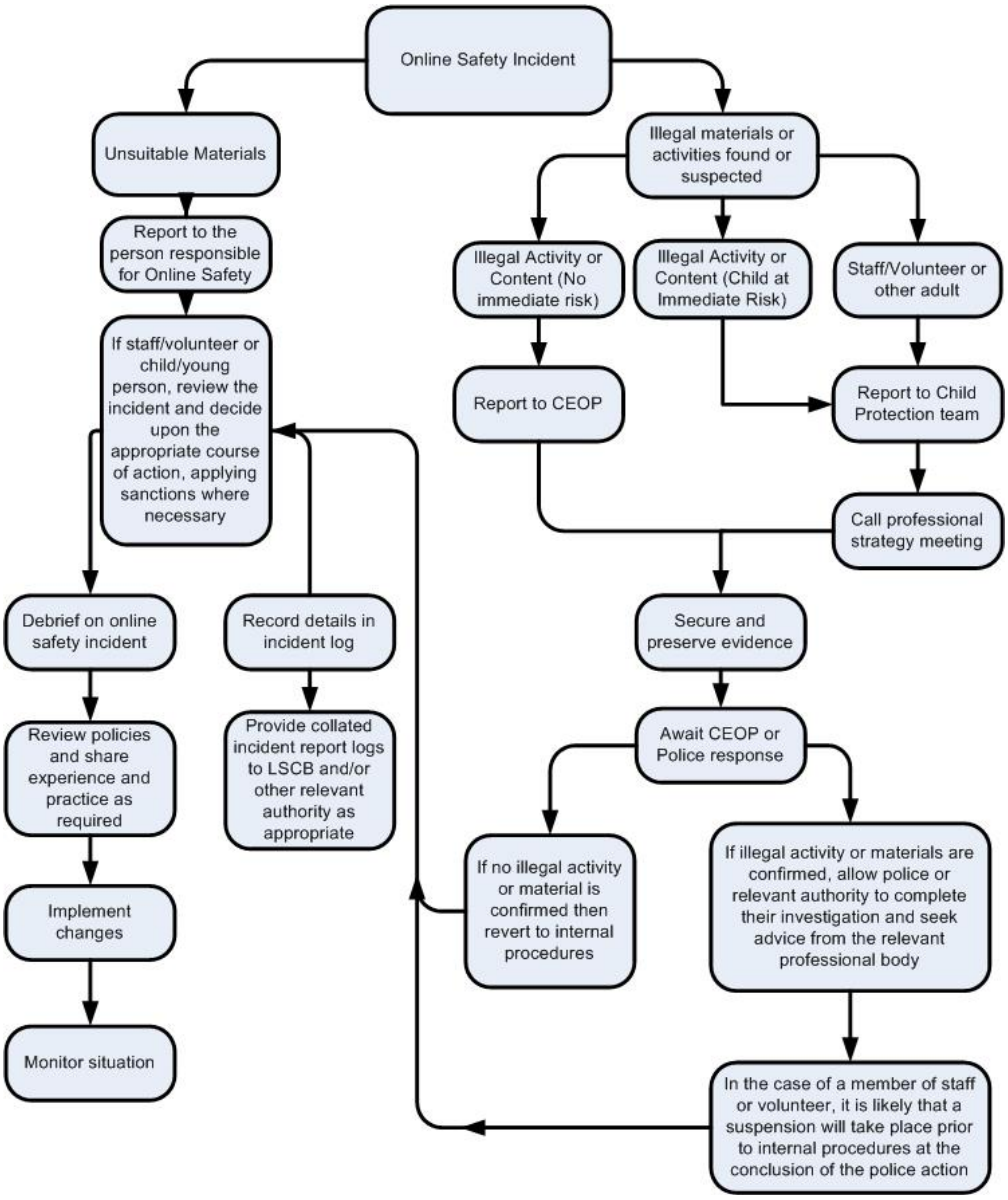
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			x			
On-line gaming (non educational)					x	
On-line gambling					x	
On-line shopping / commerce			x			
File sharing			x			
Use of social media			x			
Use of messaging apps			x			
Use of video broadcasting eg YouTube			x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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 procedures (see behaviour policy).

Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Phase leader	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X		X	
Unauthorised use of non-educational sites during lessons		X							
Unauthorised use of mobile phone / digital camera / other mobile device		X	X						
Unauthorised use of social media / messaging apps / personal email		X							
Unauthorised downloading or uploading of files		X							
Allowing others to access school network by sharing username and passwords		X							
Attempting to access or accessing the school network, using another student's / pupil's account		X							
Attempting to access or accessing the school network, using the account of a member of staff		X	X						
Corrupting or destroying the data of other users		X	X			X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X		X	
Continued infringements of the above, following previous warnings or sanctions		X	X			X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X			X			
Deliberately accessing or trying to access offensive or pornographic material			X			X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X			X	X		X

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email		X	X					X
Unauthorised downloading or uploading of files		X	X					
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X	X			X		
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X	X					X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X				X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X	X	X				X
Actions which could compromise the staff member's professional standing		X	X					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X					
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X					X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X					
Breaching copyright or licensing regulations		X	X					
Continued infringements of the above, following previous warnings or sanctions		X	X					X

Monitoring of this Policy (to be agreed)

This Online Safety policy has been reviewed by a working group made up of:

- Headteacher
- Senior Leadership
- ICT Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governing Board

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	
The implementation of this Online Safety policy will be monitored by the:	
Monitoring will take place at regular intervals:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

Considerations:

- Is it possible to separate online safety role to ICT as they are both so large?
- Can staff receive encrypted memory sticks for transferring date / completing reports etc on out of school systems?

<u>Concern reporting log</u>

Reporting Log

Group: ……………………………………………………………………………………………

Date	Time	Incident	Action Taken		Incident Reported by	Signature
			What?	By Whom?		

Acceptable Use Policy

The aim of this Acceptable Use Policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet and email use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

The AUP should be read carefully to ensure that the conditions of use are accepted and understood.

This version of the AUP was created in January 2014 and reviewed May 2017.

School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions will always be supervised by a member of staff.
- Filtering systems are used by our Internet Service Provider, in order to minimise the risk of exposure to inappropriate material.
- The internet Service Provider will monitor Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software is present on all machines and is updated and checked automatically on a daily basis.
- The use of personal memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

World Wide Web

- School staff and pupils will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- School staff and pupils will report accidental accessing of inappropriate materials in accordance with school procedures.
- Pupils will use the Internet for educational purposes only.
- Pupils will not copy information into work without acknowledging the source (plagiarism and copyright infringement).
- Pupils will **NEVER** disclose or publicise personal information.
- Downloading materials or images not relevant to class work and homework is in direct breach of the school's acceptable use policy.
- School staff and pupils will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

- School staff and pupils will use approved email accounts.
- School staff and pupils will not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

- Pupils will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Pupils will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Pupils will note that sending and receiving email attachments is subject to permission from their teacher.

Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication forums that have been approved by the school, e.g. within a Learning Platform.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

School Website

- The website will be checked to ensure that they do not contain personal details.
- The publication of pupil work will be co-ordinated by school staff.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission. Video clips may be password protected.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will not publish the surnames of any pupils.
- The school will ensure that the image files are appropriately named – will not use pupils' names in image files if published on the web.
- Pupils will continue to own the copyright on any work published.

Personal Devices

Pupils are prohibited from bringing personal devices into school.

Support Structures

The school will inform pupils and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet may result in disciplinary action, using the behaviour policy in place in school, including written warnings, withdrawal of access privileges and, in extreme cases, exclusion. The school will report any illegal activities to the appropriate authorities.

Edwards Hall Primary School
Pupil Acceptable Use

Agreement / eSafety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet anyone.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Edwards Hall Primary School

Dear Parent/ Carer,

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

- Internet sessions will always be supervised by a member of staff.
- Filtering systems are used by our Internet Service Provider, in order to minimise the risk of exposure to inappropriate material.
- The internet Service Provider will monitor Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software is present on all machines and is updated and checked automatically on a daily basis.
- The use of personal memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission.
- **Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.**

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school office.

Parent/ carer signature
We have discussed this and ……………………………………..........(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Edwards Hall Primary School.

Parent/ Carer Signature …….…………………..……………………….

Class …………………………………. Date ………………………………