ESAFETY POLICY

BACKGROUND AND 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 students/pupils learn from each other.

These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use.

However, the use of these new technologies can put young people at risk within and outside the school.

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

DEVELOPMENT / MONITORING / REVIEW OF THIS POLICY

This E-Safety Policy has been developed in consultation with

- School Child Protection Officer
- School Leadership Group
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers
- Community users

Consultation with the whole school community has taken place through the following:

- Student/Pupil Council
- INSET
- Governors' Committee meetings
- School website / newsletters

SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW

This E-Safety Policy was first approved by Full Governors Committee on Wednesday 4 December 2013.

The implementation of this E-Safety Policy will be monitored by the School Leadership Team and the school's ICT Systems Manager annually, during the Autumn Term.

The Governors will receive a report on the implementation of the E-Safety Policy generated by the monitoring group at least once a year.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Should serious e-safety incidents take place, advice from the Local Authority, including safeguarding teams and, if necessary, the police, will be sought.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Logs of all internet activity via the Internal Filtering System
- Internal monitoring data for network activity

SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, students, 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 Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

ROLES AND RESPONSIBILITIES

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

GOVERNORS:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Link Governor.

HEADTEACHER AND SCHOOL LEADERSHIP TEAM:

- The Headteacher 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 Coordinator (Sian Elcomb/Imtiaz Dalal)
- The Headteacher and another member of the School 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.
- The Headteacher and the School Leadership Team (SLT) are 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 Headteacher and the School Leadership Team (SLT) will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The School Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-SAFETY COORDINATOR:

- 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 the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety Governor to discuss any current issues
- attends relevant meetings of Governors' committees
- reports regularly to School Leadership Team

ICT TECHNICAL STAFF:

The ICT Systems Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets the e-safety technical requirements and Staff ICT Use Agreement and any relevant Local Authority E-Safety Policy and guidance;
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator for investigation, action and appropriate sanction.
- that monitoring software is implemented and updated

TEACHING AND SUPPORT STAFF:

Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the school Staff ICT Use Ageement;
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation;
- all digital communications with students/pupils (email / Virtual Learning Environment) should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other school activities;
- students/pupils understand and follow the school e-safety and acceptable use policy;
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra curricular and extended school activities using appropriate software where appropriate
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- in lessons where internet use is pre-planned 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.

DESIGNATED PERSONS FOR CHILD PROTECTION: (MRS ELCOMB / IMTIAZ DALAL)

DSPs should be trained in e-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

STUDENTS / PUPILS

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

PARENTS / CARERS

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

Parents and carers will be responsible for endorsing by signature the Student/Pupil 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 Acceptable Use Policy before being provided with access to school systems.

POLICY STATEMENTS:

EDUCATION: STUDENTS / PUPILS

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

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

- A planned e-safety programme should be provided as part of ICT / Citizenship / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school;
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities;
- Students/pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Students/pupils should be helped to understand the need for the student/pupil Acceptable Use Policies and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Staff should act as good role models in their use of ICT, the internet and mobile devices.
- 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, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

EDUCATION: PARENTS / CARERS

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

The school will therefore seek to provide information and awareness to parents and carers through newsletters, our website and our VLE.

EDUCATION AND TRAINING: STAFF

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

- 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 ICT Use Agreement.
- The E-Safety Coordinator or other nominated person will provide advice and guidance to individuals as requested and required.

TRAINING: GOVERNORS

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

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

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:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the LGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by The ICT Systems Manager who will keep an up to date record of users and their usernames. Staff will be required to change their password every term.
- The “master / administrator” passwords for the school ICT system, must also be available to the Headteacher or other nominated senior leader and kept in the school safe.
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by LGfL in addition to a further internal filtering system which gives greater control.
- In the event of the ICT Systems Manager (or other person) 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 Headteacher (or other nominated school leader).Any filtering issues should be reported immediately to LGfL.

- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Systems Manager and the ICT Team.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the ICT Systems Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, 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, currently Sophos.
- Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Any off-site backup of school data will be encrypted with “bank-level” security.

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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics such as racism, drugs, and discrimination that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students/pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

USE OF DIGITAL AND VIDEO IMAGES - PHOTOGRAPHIC, VIDEO

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students/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 students/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.
- 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 there own personal use (as such use is 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 students/pupils in the digital / video images.
- 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 students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers relating to school use of photographs of students/pupils is obtained as part of the registration process when children are admitted to the school
- Where a family has refused permission for their child's photograph to be used, it is the responsibility of that child to indicate beforehand to the relevant member of staff or authorised adult taking photographs that they do not wish to be included. These requests will always be respected.
- Students' and Pupils' work can only be published with the permission of the students/pupils 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.

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
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimizing 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, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

COMMUNICATIONS

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. Staff, students/pupils should therefore use only the school email service to communicate with others.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to E-safety Co-ordinator – 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, students/pupils or parents / carers (email, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

	Staff & Students			Pupils				
Communication Technologies	Not Allowed	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at certain times	lowed with staff permission	Not allowed
Mobile phones may be brought to school		X		X				
Use of mobile phones in lessons	X			X				
Use of mobile phones in social time		X		X				
Taking photos on mobile phones / cameras	X			X				
Use of other mobile devices eg tablets, gaming devices		X		X				
Use of personal email addresses in school, or on school network		Staff only X		X				
Use of school email for personal emails	X			X				
Use of messaging apps		X		X				
Use of social media		X		X				
Use of blogs		X		X				

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

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

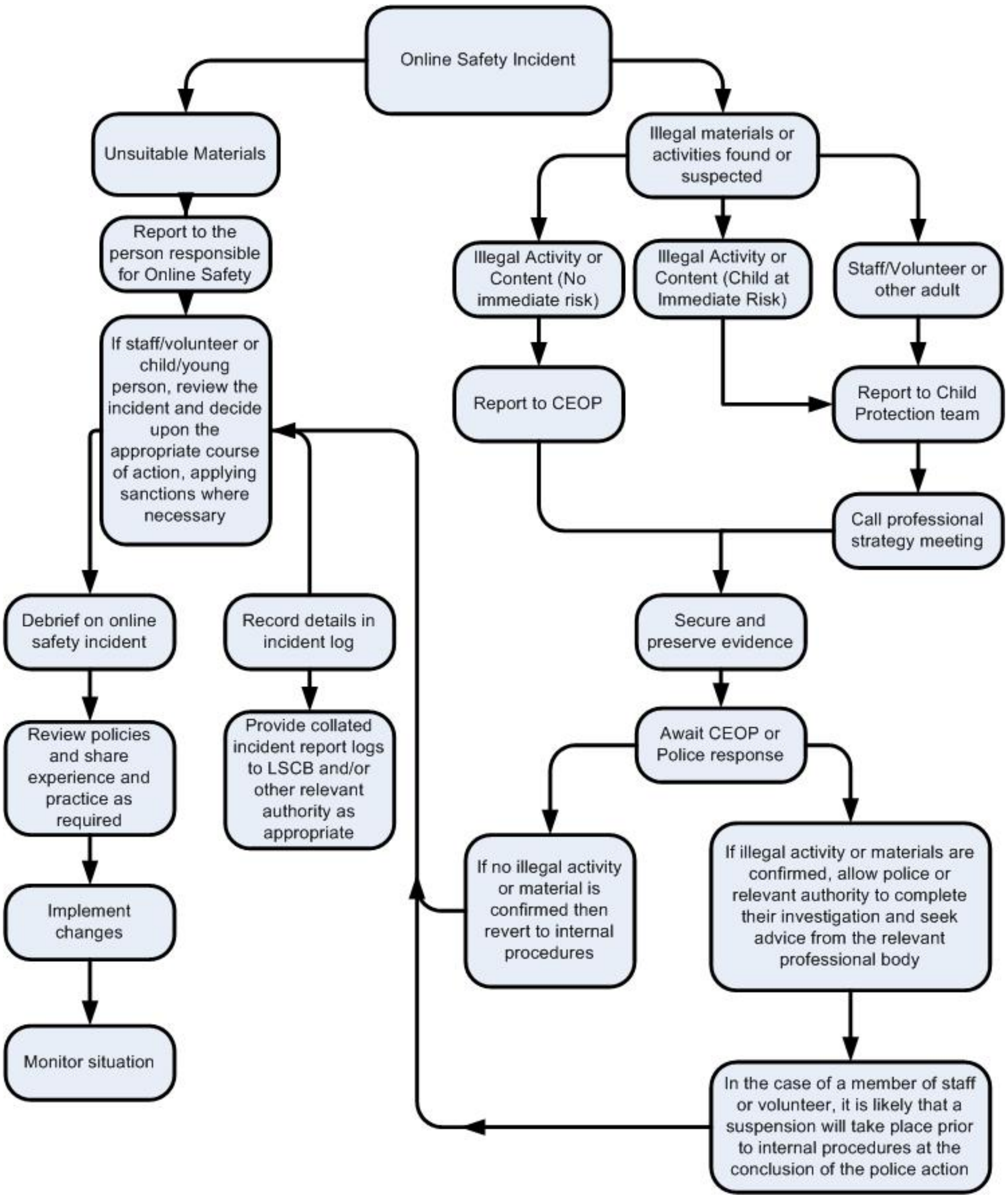
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse 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 egYoutube				X		

RESPONDING TO INCIDENTS OR 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.

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 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 / academy 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 / disciplinary procedures as follows:

Students/Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Pastoral	Refer to SLT	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Refer to ICT\Removal of network / internet access rights	Verbal 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				X		X	
Unauthorised use of mobile phone / digital camera / other mobile device		X				X		X	
Unauthorised use of social media / messaging apps / personal email		X		X		X		X	X
Unauthorised downloading or uploading of files		X				X	X	X	
Allowing others to access school network by sharing username and passwords		X				X	X	X	
Attempting to access or accessing the school network, using another student's / pupil's account		X				X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff		X	X		X	X	X	X	
Corrupting or destroying the data of other users		X			X	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	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X			X		X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		X	X
Using proxy sites or other means to subvert the school's filtering system		X				X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X						X	
Deliberately accessing or trying to access offensive or pornographic material		X	X	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

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to School Business Manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action / filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	X	X	X	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				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	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	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		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X	X			X	X	X
Actions which could compromise the staff member's professional standing		X	X	X			X		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X	X				X		X
Using proxy sites or other means to subvert the school's / academy's filtering system		X	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				X	X	X
Breaching copyright or licensing regulations	X	X				X	X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X				X	X	X

Review Date	By Whom	Changes
November 2014		

Signed by: …………………………… Date: ………………………….. on behalf of the Governing Body.