Online Safety Policy December 2017

Governors' Committee Responsible:	Children and Learning, Safeguarding
Governor Lead:	Mr. Anthony Clark
Nominated Lead Member of Staff:	Manjeet Rebello
Deputy DCPO:	Rachel Nicholls
Status & Review Cycle:	Statutory Annual
Next Review Date:	September 2018

Overview

This e-safety policy has been developed by a working group made up of:

- School E-Safety Coordinator
- Headteacher
- Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers
- Community users

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

- Staff meetings
- School Council and Digital Leaders
- INSET Day
- Governors meeting
- Parents evening
- School website/newsletters

SCOPE OF POLICY

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

The Education and Inspections Act 2006 empowers 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 e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Schedule for Development, Monitoring and Review

This Online Safety policy was approved by the Governing Body on:	
The implementation of this e-safety policy will be monitored by the:	E-Safety Coordinator
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) 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 e-safety or incidents that have taken place. The next anticipated review date will be:	September 2018
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	GLF ICT Manager, LA Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Internal monitoring data for network activity.
- Surveys/ questionnaires of pupils, parents/ carers and staff.
- Parent and Family forum/ workshops.

ROLE 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 Online-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. The members of the Governing Body in charge of Safeguarding and Children and Learning will also be responsible for overseeing Online Safety. Their roles will include:

- regular meetings with the E-safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meeting

HEADTEACHER AND SENIOR LEADERS:

The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online will be delegated to the E-Safety Co-ordinator.

- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- Through performance management of the E-Safety Co-ordinator, the Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and another member of the Senior Management 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 CO-ORDINATOR:

- leads e-safety
- 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 Safe guarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

NETWORK MANAGER/TECHNICAL STAFF:

The Network 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 outlined in the GLF Security Policy and Acceptable Usage Policy.
- that users may only access the school's networks through a properly. enforced password protection policy, in which passwords are regularly changed.
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

- that the use of the network/email is regularly monitored in order that any misuse/ attempted misuse can be reported to the E-Safety Co-ordinator/Headteacher for investigation.
- that monitoring systems are implemented and updated as agreed in school policies.

TEACHING AND SUPPORT 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 Acceptable Use Policy.
- they report any suspected misuse or problem to the E-Safety Co-ordinator/Headteacher for investigation.
- digital communications with pupils (e.g. email) should be on a professional level and e-safety issues are embedded in all aspects of the curriculum and other school activities.
- pupils understand and follow the school e-safety and acceptable use policy.
- 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.
- 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 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.

CHILD PROTECTION OFFICER

- should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:
- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.

- cyberbullying.

PUPILS:

• are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (at KS1 parents/carers will sign on behalf of the pupils).

• 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 cyberbullying.

• 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 and the school website. Parents and carers will be responsible for:

• endorsing (by signature) the Pupil Acceptable Use Policy.

• accessing the school website in accordance with the relevant school Acceptable Use Policy.

COMMUNITY USERS:

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

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 e-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 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 Computing, PSHE and 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 E-safety day, assemblies and workshop activities.

1. As part of our committed to placing the Convention of the Rights of the Child at the heart of our ethos and practice enabling us to ensure the children in our school community are safe and protected; we adhere to the Articles from the Convention of the Rights of the Child (CRC). As a school we are committed to teaching our children about E-Safety and giving children responsibility and ownership of their online practice. Pupils have the right to access reliable information (Article 17), whether that is through print media, television or online. Young people increasingly use the internet to learn, play and socialise. It is vital, therefore, that they can take advantage of all the internet has to offer in a safe, informed way while respecting their right to privacy (Article 16) and their right to protection (Article 19).
2. Audley's Digital Leaders will have a key pupil voice in guiding their peers to be safe online.

3. 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 helped 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 the internet and mobile devices both within and outside school.

EDUCATION – PARENTS/CARERS

PARENTAL SUPPORT

Parents will need:

- To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren
- To consult with the school if they have any concerns about their children's use of technology
- to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images.

Parents may either underestimate or 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. "There is a generational digital divide"(Byron Report).

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

- Letters, newsletters and the school website.
- Parent workshops/ forum

- Parent Info.
- Reference to CEOP's 'Thinkuknow' website

EDUCATION – EXTENDED SCHOOLS

The school will offer family learning workshops in e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the digital world.

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 Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through attendance at training sessions and by reviewing guidance documents released by LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice, guidance or training as required by individuals.

TECHNICAL – EQUIPMENT, FILTERING AND MONITORING

The school will be responsible for ensuring that the school 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 and iPad systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the GFL 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. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Coordinator
- All users (year 1 and above) will be provided with a username and password by (insert name or title) who will keep an up to date record of users and their usernames.
- The "master/administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by GLF.
- The school has provided enhanced user-level filtering through the use of the GLF filtering programme (See GLF Acceptable Use Policy).
- In the event of the Network Manager 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).
- Any filtering issues should be reported immediately to GLF.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Coordinator.

- 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.
- An appropriate system is in place (email/ phone access to an e-ticket) for users to report any actual/potential e-safety incident to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

CURRICULUM

E-safety should be a focus in ***all areas*** of the curriculum and staff and Digital Leaders should reinforce e-safety messages in the use of ICT across a progressive and age appropriate curriculum.

- 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, 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 (eg 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.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

USE OF DIGITAL AND VIDEO IMAGES – PHOTOGRAPHIC AND VIDEO

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must adhere to the parent's disclaimer and 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.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission in the form of a disclaimer from parents or carers will be obtained before photographs of pupils are published on the school website/ twitter.

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 14
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

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, 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.

The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff and other adults				**Pupils**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones or other camera devices				✓				✓
Use of hand held devices eg PDAs, PSPs				✓			✓	
Use of personal email addresses in school, or on school network			✓					✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging		✓						
Use of social networking sites		✓						✓
Use of blogs	✓						✓	

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 and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and pupils or parents / carers (email, twitter) must be professional in tone and content.
- Whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.
- 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 ACTIVITES

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 certain internet usage as follows:

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:	**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
child sexual abuse images					✓
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
adult material that potentially breaches the Obscene Publications Act in the UK					✓
criminally racist material in UK					✓
pornography				✓	
promotion of any kind of discrimination				✓	
promotion of racial or religious hatred					✓
threatening behaviour, including promotion of physical violence or mental harm					✓

any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by GFL and the school			✓		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)	✓				
On-line gaming (non educational)		✓			
On-line gambling				✓	
On-line shopping / commerce		✓			
File sharing		✓		✓	
Use of social networking sites				✓	
Use of video broadcasting e.g. Youtube		✓			

RESPONDING TO INCIDENTS OF MISUSE

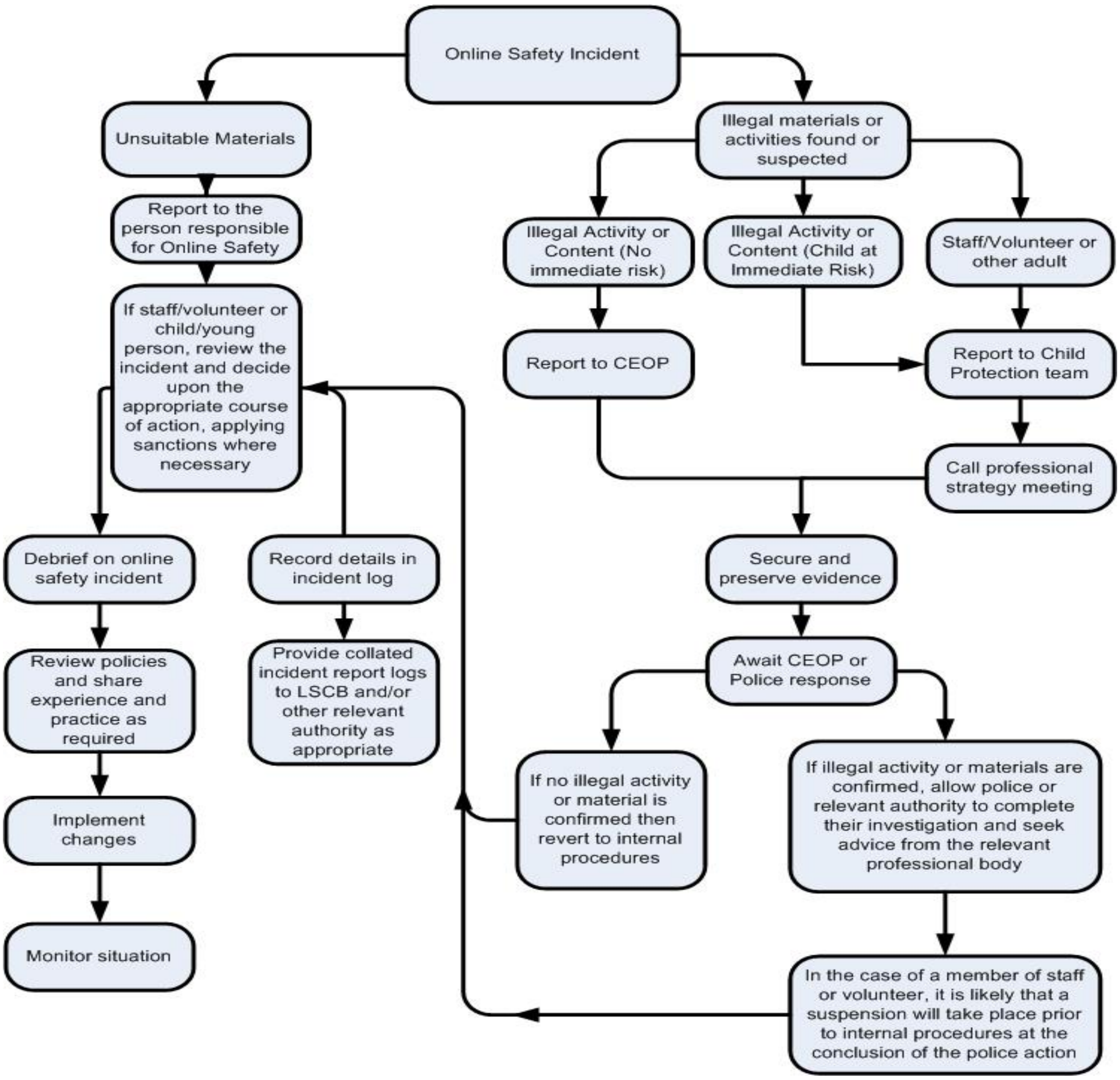
We hope that all members of our school community will be trusted, responsible users of ICT; who adhere by this policy. However, there may be times when infringements of the policy could take place.

(Please refer to the Legislation- Regulation of Investigatory Powers Act 2000, Malicious Communications Act 1988)

If any apparent or actual misuse appears to involve illegal activity i.e..

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart below should be consulted and actions followed in line with the SWGfl flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



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

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. It is intended that incidents of misuse will be dealt with through normal Audley Behaviour Policy procedures as follows:

Pupils	Action/ Sanctions

Incidents:	**Refer to class teacher**	**Refer to Headteacher**	**Refer to Police**	**Inform parents/carers**	**Removal of network/internet**	**Warning**	**Further sanction e.g. suspension/ 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		x
Unauthorised use of non-educational sites during lessons	X					X	
Unauthorised use of mobile phone/ digital camera/other handheld device	X					X	
Unauthorised use of social networking/ instant messaging/personal email	X					X	
Unauthorised downloading or uploading of files	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 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		
Corrupting or destroying the data of other users	X	X		X	X		
Sending an email, text or instant 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
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	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		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		

STAFF	**Action/ Sanctions**

Incidents:	**Refer to performance manager**	**Refer to Headteacher**	**Refer to Local Authority**	**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
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email		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 e.g. holding or transferring data in an insecure manner		x			x	x		
Deliberate actions to breach data protection or network security rules		x				x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x						x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x				x	x	x
Using personal email/social networking/texting for digital communications with pupils		x						
Actions which could compromise the staff		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
Using proxy sites or other means to subvert the school's filtering systems		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
Breaching copyright or licensing regulations		x				x		
Continued infringements of the above, following previous warnings or sanctions		x						x

ACCEPTABLE USE POLICIES

Acceptable Use Policy (AUP): PUPIL Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students* / *pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school / academy* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/ internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student / Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

• I use the school ICT systems and equipment (both in and out of school)

• I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc

• I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, website etc.

Name of Pupil:

Class:

Signed*

Date:

* If you are the parent of a KS1 pupil, please sign on their behalf.

ICT and Acceptable Use Policy (AUP): Staff Agreement

This policy covers the use of digital technologies in school: email, Internet, network resources, learning platform, software, handheld devices, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system (Office 365) for any school business.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network/Internet that does not have up-to-date anti-virus software.
- I will not use personal digital cameras or any device with camera capabilities for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with or associated with my professional role or the school.
- I agree and accept that any computer, laptop, handheld device (including iPad) loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and

confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed the school's e-safety curriculum into my teaching.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

iPad Acceptable Use Policy for Audley Primary School
User Responsibilities

- The iPad screen is made of glass and is therefore subject to cracking and breaking if misused; neverdrop or place heavy objects (book, laptops etc) on top of the iPad.
- The iPad must be kept in its protective case at all times.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extreme temperatures.
- Do not store or leave unattended.
- Users may not photograph any other person without that person's consent
- Photographs of children must be in line with Consent Letter Agreement
- The whereabouts of the iPad should be known at all times.
- It is a user's responsibility to keep their iPad as safe and secure as possible.
- Images of other people may only be made with the permission of the person, or parents of theperson, in the photograph.
- Upon returning the iPad to the school, it is the user's responsibility to delete all personal materials,including pictures, passwords and e-mails from the device.
- The iPad is a school tool designed to enhance practice. It is not for personal use.
- If the iPad is lost, stolen or damaged, the Computing Co-Ordinator, ICT Technician or Head Teachermust be informed immediately

User Agreement / Signature

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

I agree to abide by all the points above.

I wish to have an email account; be connected to the Internet; be able to use the school's ICT resources and systems.

Signature ………………………………………………… Date:

Full Name .... (printed)

Job title ....

One copy retained by member of staff , second copy for school file

Acceptable Use Policy (AUP): PARENT/CARER Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name:	
Pupil Name:	

As the parent/carer of the above *pupils*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed