Arnold Mill Primary School

Internet & Online Safety Policy

May 2024

Approved by:	S&P Committee
Last Review Date:	May 2024
Next Review Date	May 2025

1. Aims

Arnold Mill Primary school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Ensure the teaching of our SMART rules is planned for and taught regularly throughout KS1
- Ensure the teaching of the 5 pillars of Be Internet Legends is planned for and taught regularly throughout KS2.
- Ensure that the Keeping Children Safe in Education document and the UK Council for Internet Safety's framework (Education for A Connected World) are at the heart of our teaching.
- Deliver an effective approach to internet safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and Guidance

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 IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers the Headteacher 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 internet 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 policy also takes into account the National Curriculum computing programmes of study.

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.

3. Roles and Responsibilities

3.1 The Governing Board

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Online safety Governor. The role of the Online safety Governor will include:

- regular meetings with the Online safety Co-ordinator/computing leadership team
- regular monitoring of online safety incident logs
- reporting to relevant Governors

3.2 The Headteacher

- 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 computing leadership team.
- The Headteacher and (at least) another member of the Senior Leadership Team and Computing 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 is responsible for ensuring that the Computing leaders and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- 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.
- Take day to day responsibility for internet and online safety issues.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an internet/online safety incident taking place.

3.3 Staff

- Must have an up to date awareness of internet and online safety matters and of the current school internet safety policy.
- Must have read, understood and signed the Staff Acceptable Usage Policy.
- Report any suspected misuse or problem to the Headteacher.
- Should only communicate onlinely with pupils/parents/carers on a professional level and only carry this out using official school systems (school phone or school email).
- Have internet and online safety issues embedded in all aspects of the curriculum and other activities – through the Project Evolve scheme of work.
- Explicitly teach the SMART rules (KS1) and Be Internet Legends Pillars (KS2) to ensure children have a secure understanding.
- Ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (upper KS2).
- Monitor the use of online technologies, mobile devices, cameras etc. in lessons and other school activities.
- Should plan ahead for lessons where internet use is required so that websites can be checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches (Red Button).
- Should report online safety incidents via CPOMS.

3.4 Pupils

- Are responsible for using the school online technology systems appropriately and sensibly.
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (upper KS2 children).

- Should know the importance of reporting any worries, abuse, misuse or access to inappropriate materials and know how to do so (Using the red button, following the SMART/B.I.L. rules).
- Will be expected to know and understand policies on the use of mobile devices.
- They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good internet and online safety practice when using online technologies out of school.

3.5 Computing Leaders

- Provide training and advice for staff.
- Liaise with school technical staff – IT Technicians (WHT).
- Report any updates to other staff – through staff meetings and minutes or emails.
- Have a leading role in establishing and reviewing the school internet and online safety policies/documents.

3.6 Network Manager/Technical Staff

- Ensure the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensure the school meets required internet and online safety technical requirements and any Local Authority/Guidance.
- Make staff aware that they may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed e.g. staff are requested to change laptop passwords regularly, only access school/pupils documents on the system on the school premises.
- 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.
- Ensure that the use of the network/internet/email is regularly monitored so that any misuse/attempted misuse can be reported to the Headteacher and Computing Leaders.
- Ensure that monitoring software/systems are implemented and updated as agreed in school policies.

3.7 Designated Safeguarding Lead

Designated Safeguarding Leads 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

3.8 Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the importance of online/online safety. 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/literature. 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:

- online and video images taken at school events
- access to parents' sections of the website/VLE and on-line student/pupil records

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Keeping children safe online- Safer schools website and APP

4. Educating Pupils about Online Safety

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be 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/PSHE/other lessons and should be regularly revisited – taught discretely through PSHE, online literacy and the computing curriculum.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities – online safety assemblies and online safety day in February.
- 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 online 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. Google safe search is implemented to limit contents and Hector the Protector is on all laptops.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

5. Educating Parents about Online Safety

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, website
- Parents'/Carers' evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers Safer schools APP
- The school website will provide online safety information for the wider community

6. 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.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- 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 (e.g. school safe).
- ICT services are 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 (including child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school has provided enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- 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.
- An agreement is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

7. Use of online and video images

The development of online 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 online images on the internet. Such images may provide avenues for cyberbullying to take place. Online 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 online 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and online images of their children at school events for their 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 pupils in the online/video images.
- Staff and volunteers are allowed to take online/video images to support educational aims using school cameras/tablets, but must follow school policies concerning the sharing, distribution and publication of those images. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking online/video images that students/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 from parents or carers will be obtained before photographs of students/pupils are published on the school website.
- Staff and pupils must not publish online, copyrighted images on the school's website or social media pages.

8. 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.
- It has a Data Protection Policy.
- 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.

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, at all times.
- 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.
- Keep mobile phones out of sight at all times whilst a pupil is or may be present.
- Brief parents or visitors in school or on trips of the 'no visible mobile phones' policy.

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

9. 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. 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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- 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 online communication between staff and pupils or parents/carers (email, chat, 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 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 online technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10. Social Media

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.

Clear reporting guidance, including responsibilities, procedures and sanctions helps school staff ensure that:

- No reference is made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not attributed to Arnold Mill or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

11. 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					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	

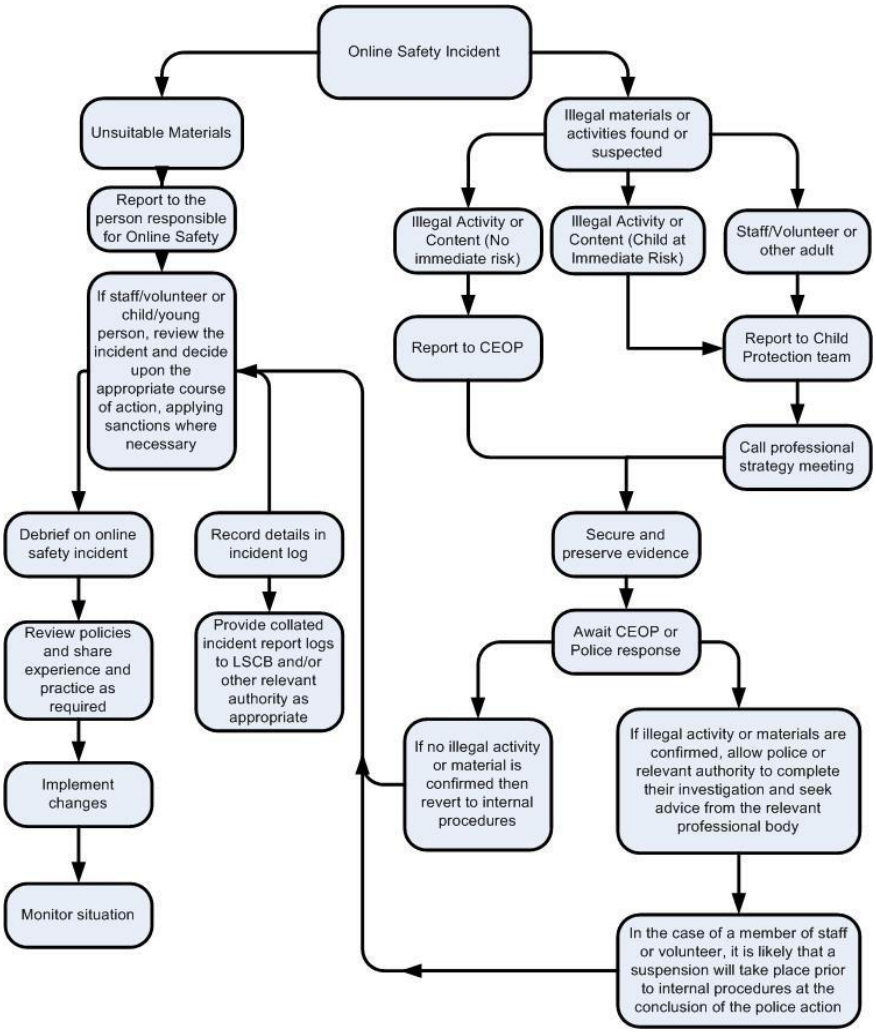
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non educational)			X		
On-line gambling				X	
On-line shopping / commerce				X	
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			x		

12. Responding to issues 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 website(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) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of online 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
  - 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	Refer to Head of Department Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / care	Removal of network / internet access rights	Warning	Further sanction e.g. 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					
Unauthorised use of non-educational sites during lessons	x	X	x					X	
Unauthorised use of mobile phone / online camera / other mobile device	X	x	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		X	
Allowing others to access school network by sharing username and passwords	x	x	x			x		X	
Attempting to access or accessing the school network, using another student's / pupil's account	x	x	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	
Continued infringements of the above, following previous warnings or sanctions	x	x	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	X	
Using proxy sites or other means to subvert the school's filtering system	x	x	x			x	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x			x		x	

Deliberately accessing or trying to access offensive or pornographic material	x	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			x		x	

13. Training

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 will be made available to staff. This will be regularly updated and reinforced.
- All new staff should 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 Computing Leaders will receive regular updates through attendance at external training events (e.g. from Redhill Alliance/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- The Computing leaders will provide advice/guidance/training to individuals as required.
- This Online safety policy will be presented to and discussed by staff through staff meetings, email or INSET days.

14. Links with other policies

- Relationship and Sex Education policy – covers online safety/grooming/sexting
- PSHE Policy – covers online safety
- Anti-Bullying Policy – covers cyberbullying

15. Monitoring

Hilary Carter & Sam Lloyd (Computing leaders) have developed this internet and online safety policy, in consultation with:

- Headteacher, Jackie Oldfield, also the online safety officer
- Staff – including Teachers, Support Staff, Volunteers
- Governors

The school will monitor the impact of the policy using:

- Logs of reported incidents via CPOMS
- Surveys/questionnaires of pupils, parents/carers and staff
- Planning scrutinies
- Learning walks and pupil conversations – checking understanding of SMART rules/B.I.L pillars

This policy will be reviewed by the Headteacher annually. At every review, the policy will be approved by the Strategic and Pastoral Governing Board.