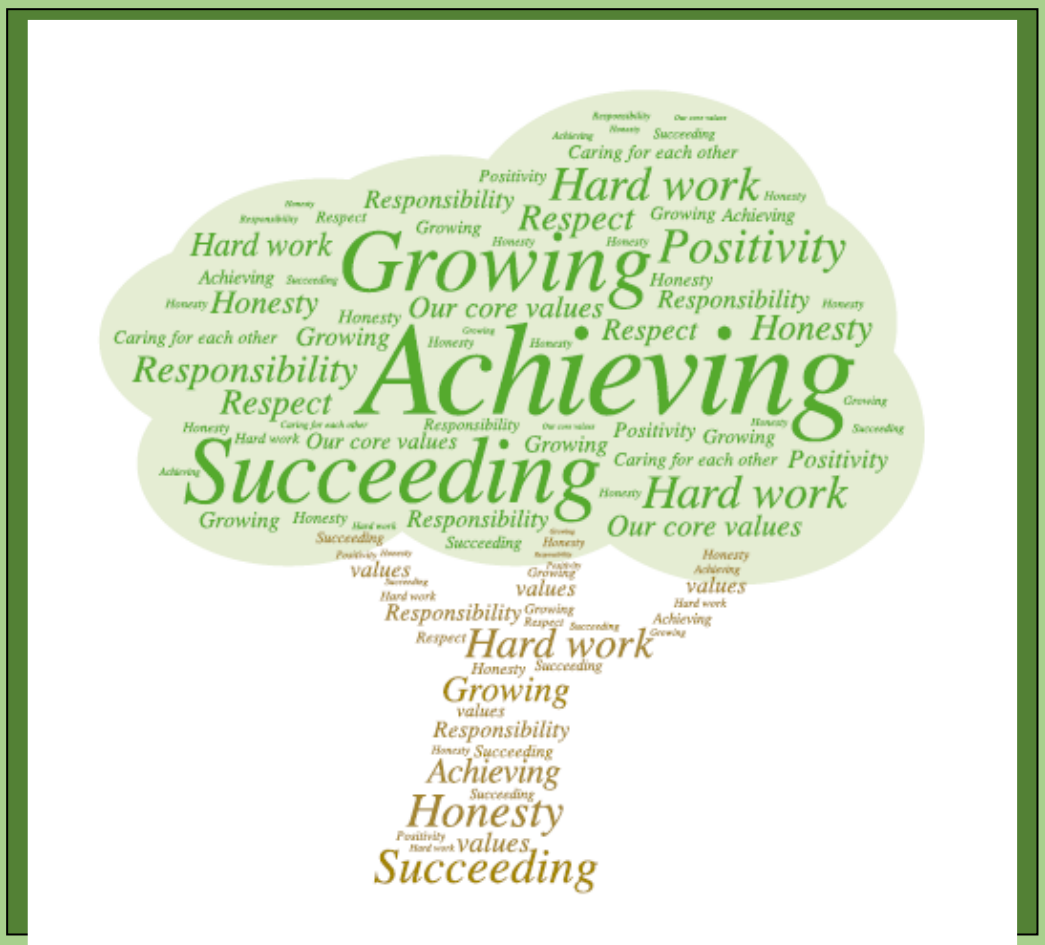
Park End Primary School



Approved By: *D. Jackson*

Date: 14.1.19

Online Safety Policy

Review Date	Type of Review	Comments	Initials
June 2017	Full	Full Review	LR
Jan 2019	Update/Review	Updated in line with GDPR regulation	KMc/LR
Jan 2019	Update	Changed ‘e-safety’ to ‘online safety’	LR

Park End Primary School

Online Safety Policy

Scope of the Policy

- This policy applies to all members of Park End Primary School (including pupils, staff, volunteers, parents, carers, visitors, community users) who have access to and are users of school systems, both in and out of Park End Primary School.

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

- Park End Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Governors receive regular information about online safety incidents and monitoring reports. The Safeguarding Governor also has the role of Online Safety Governor.

Headteacher

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community; although the day to day responsibility for online safety will be delegated to the online safety coordinator and ICT coordinator.

  - The Headteacher will receive reports of online safety incidents and these will be logged to inform future online safety developments. This data will be kept in line with the GDPR policy.
  - The Headteacher and Deputy Headteacher are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see complaints policy)

- The headteacher is responsible for ensuring that the online safety coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- 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 senior leadership team and governors will receive regular monitoring reports from the Online safety Co-ordinator.

Online safety Coordinator

- The online safety coordinator is L. Richardson, who is also the designated safeguarding lead. Her role is to:

  - take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents
  - ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
  - provide training and advice for staff
  - liaise with the Local Authority / relevant body
  - liaise with school technical staff where necessary
  - meet regularly with the Online safety Governor to discuss current issues and review incident logs
  - report regularly to Senior Leadership Team

Technical staff

- Park End Primary School has a managed ICT service provided by an outside contractor; it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. The managed service provider is fully aware of Park End Primary School online safety policy and procedures.

- The technician assigned to the school by the outside contractor is responsible for ensuring

  - that Park End Primary School's technical infrastructure is secure and is not open to misuse or malicious attack
  - that Park End Primary School meets required online safety technical requirements according to Middlesbrough Local Authority Guidance.
  - that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

- the filtering system (Smoothwall) is applied and updated on a regular basis.

- that the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the headteacher and online safety coordinator for investigation or data protection officer in the case of a misuse of data.

- that monitoring software and systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

- Teaching and support staff are responsible for ensuring that:

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

Designated Safeguarding Lead

- The designated safeguarding lead should be trained in online safety issues and be aware of the potential for serious child protection and other safeguarding issues to arise from:

  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- cyber-bullying

Pupils

- Pupils must

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

Parents / Carers

- Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Park End Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local online safety campaigns and 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:

  - digital and video images taken at school events
  - access to parents' sections of the website and on-line pupil records
  - their children's personal devices in the school

Reviewing this Policy

- This online safety policy will be reviewed annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. This policy will also be reviewed in light of the GDPR regulation.

- Consultation with the whole school community will take place through a range of formal and informal meetings.

- The school will monitor the impact of the policy using:
    - Logs of reported incidents
    - Monitoring logs of internet activity (including sites visited)
    - Internal monitoring data for network activity
    - Surveys / questionnaires of pupils, parents, carers and staff

Policy Statements

Education – pupils

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

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

- Online safety is taught as part of the computing curriculum and PSHE lessons (jigsaw).

- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities.

- Pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils will 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 will act as good role models in their use of digital technologies, the internet and mobile devices.

- In lessons where internet use is pre-planned, it is best practice that pupils are 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 will 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 (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 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

- Parents and carers play an essential role in the education of their children and in the monitoring and 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:
    - Letters, newsletters, web site.
    - Parents / Carers evenings / sessions
    - High profile events and campaigns e.g Safer Internet Day
    - Reference to the relevant web sites and publications

Education – staff/ volunteers

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

    - Online safety training will be made available to staff during staff meetings and through CEOP. This will be regularly updated and reinforced.
    - All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
    - The online safety coordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
    - This online safety policy and its updates will be presented to and discussed by staff in staff and team meetings and other PD days.
    - The online safety Coordinator (or other nominated person) will provide advice, guidance and training to individuals as required.

Education – Governors

- Governors will take part in online safety training through participation in school training and information sessions e.g. assemblies.

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 ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Park End Primary School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by One IT Services & Solutions who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. These will be stored in accordance with the GDPR policy.

- Janet Wainwright, School Business Manager, is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

- Internet access is filtered for all users through the use of smoothwall, an additional and separate filtering system to the one provided by the broadband provider. School also use an additional system called Esafe.

- Any actual or potential technical incident or security breach is reported to the technician through the helpdesk.

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

Use of digital and video images

- The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- Photographs and video images of individual students and staff are classed as personal data and the use of such images by the school will only be with the consent of the individual concerned as well as their parent/carer. Verbal consent will not be accepted under any circumstance. If prior written consent is not given then individual images will not be used. A parent or carer has the right to refuse or withdraw their consent at any time. If a parent or carer gives partial or restricted consent, the school will comply with this.

- 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others without their permission and in line with GDPR policy.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- Particular care will be taken by school staff when considering the publication of material on the internet and in particular n the school website. Articles will be screened carefully to ensure that students cannot be individually identified by name or by any other means. This includes ensuring that they cannot be identified from the file name of any electronic image files that are placed on the school website. There are alternative strategies that the school may use, including general shots e.g. classrooms and group activities which would include relatively small images of groups of students. "Over the shoulder" can replace "passport style" photographs but still convey the activity.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Communication Technologies

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 headteacher, 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 emails between staff and pupils or parents / carers 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 at KS2 will be provided with individual school email addresses for educational use.
- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Staff will use the secure feature in the subject box when sending emails.

	Staff & other adults				Pupils				
Communication Technologies	Allowed	Not allowed	Allowed at certain time	Allowed for selected staff	Allowed	Not allowed	Allowed at certain times	Allowed with Headteacher permission
Personal mobile phones may be brought to school	X					X		X

Use of mobile phones in lesson times		X					X		
Use of mobile phones in social time			X				X		
Taking photos on personal mobile phones		X					X		
Use of other personal mobile devices e.g. tablets			X					X	X
Use of personal email addresses in school, using own mobile device			X				X		
Use of personal email for school business		X					X		
Use of messaging apps (except those adopted by school)			X				X		
Use of social media			X				X		

Social Media - Protecting Professional Identity

- Park End Primary School has a duty of care to provide a safe learning environment for pupils and staff. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm are in place**.**

- This policy should be read in accordance with the school social networking policy and DR policy.

- The school provides the following measures to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

  - Training upon acceptable use; social media; data protection and reporting issues e.g. CEOP training.
  - Clear reporting guidance, including responsibilities, procedures and sanctions
  - Risk assessment, including legal risk

- School staff should ensure that:
  - No mention is made in social media of pupils, including ex pupils, parents / carers or school staff.

- They do not engage in online discussion about matters relating to school and members of the school community.
- Personal opinion is not attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

- The school's use of social media for professional purposes will be checked regularly by the school business manager and online safety committee to ensure compliance with the Social Media and GDPR Policy.

Unsuitable / inappropriate use of school equipment.

- The school believes that the activities referred to in the following section are 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 through remote access. The use of school devices is the responsibility of the member of staff. Passwords should not be shared which would allow other people to access school equipment.

- **User Actions**

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, posts, 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
	Downloading terrorist and extremist material from the internet					x
	promotion of any kind of discrimination				x	

	threatening behaviour, including promotion of physical violence or mental harm				x	
	pornography				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 (e.g. 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. You tube that has been checked by the member of staff for suitability prior to use.	x					

Responding to incidents of misuse

- Any incidents of misuse will be referred to the Headteacher and Middlesbrough guidelines followed for misuse will be adhered to (see document entitled Misuse of school systems and devices)

School Actions & Sanctions

- It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of

the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures as follows:

Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher	Refer to Computing co-ordinator	Refer to Headteacher / Safeguarding Lead	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion	Online safety curriculum/ teaching
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
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					
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	
Corrupting or destroying the data of other users	x	x								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			x			x			x	x

Continued infringements of the above, following previous warnings or sanctions			x			x	x		x	
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		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
Accessing or downloading terrorist information (Prevent)			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

Possible Actions / Sanctions

Incidents	Refer to line manager	Refer to Headteacher	Refer to Safeguarding Lead	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Disciplinary Action	Suspension	Additional Training in online safety
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	x
Inappropriate personal use of the internet / social media / 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 or attempting to access or accessing the school network, using another person's account	x					x	x	x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner	x								
Deliberate actions to breach data protection or network security rules		x				x	x	x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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
Using personal email / social networking /		x	x	x		x	x	x	x

instant messaging / text messaging to carrying out digital communications with students / pupils									
Actions which could compromise the staff member's professional standing		x							
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x				x			
Using proxy sites or other means to subvert the school's filtering system		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	
Breaching copyright or licensing regulations	x								
Continued infringements of the above, following previous warnings or sanctions		x	x	x	x	x	x		

Appendix

- This policy should be read in conjunction with the following school policies/documents:

  - Bullying (including cyber bullying)
  - Behaviour
  - GDPR Policy
  - Privacy Policy
  - Safeguarding statement
  - Safeguarding Policy (Child protection)
  - Staff Code of Conduct
  - Staff Acceptable Use Policy
  - Child Acceptable Use Policy
  - Social Networking
  - Home/School Agreement
  - Guidance for misuse of school systems and devices

Legislation

42. This policy should be read in conjunction with the following legislation:

  - Searching, Screening and confiscation: Advice for headteachers, school staff and governing bodies (2014) DfE