The Avenue Infant School

ONLINE SAFETY POLICY

(INCLUDING ACCEPTABLE USE POLICIES)

Signed on behalf of the Governing Body: M Ryan

Position: Chair

Date: 17.5.17

Review date: May 2018

The Avenue Infant School

Online Safety Policy

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

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

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

Policy Statement

For clarity, the online safety policy uses the following terms unless otherwise stated:

Users – refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents and Carers - any adult with a legal responsibility for the child/ young person outside the school. E.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences school trips etc.

Wider school community – students, all staff, governing body, parents, clubs.

Safeguarding is a serious matter: at The Avenue Infant School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

1. To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.

2. To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the school's website; upon review all members of staff will sign as read and understand, and agree to follow both the online safety policy and the Staff Acceptable Use policy.

A copy of this policy and the student's acceptable use policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the internet.

Roles and Responsibilities

Governing Body

The governing body is accountable for ensuring that out school has effective policies and procedures in place: as such they will:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing these incidents.
- Appoint one governor **(Mark Ryan)** who has overall responsibility for the governance of online safety at the school who will:
    - Keep up to date with the emerging risks and threats through technology use
    - Receive regular updates from the head teacher in regards to training, identified risks and any incidents.
    - Meet with the Online Safety Lead
    - Report to governors on online safety issues that arise

Head teacher and Senior Leaders

Reporting to the governing body, the head teacher has overall responsibility for online safety within our school. The day to day management of this will be delegated to a member of staff, the online safety lead, as indicated below.

The Head teacher will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, e.g. students, all staff, SLT and governing body, parents.
- The designated online safety lead has had appropriate CPD in order to undertake the day to day duties.
- The Headteacher and Senior Leaders 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.
- All online safety incidents are dealt with promptly and appropriately. The Headteacher and (at least) another member of the Senior Leadership 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 later in this policy)
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online safety Co-ordinator / Officer.

Online safety Lead

The day to day duty of online safety officer is devolved to: **Helen Morrall**

The online safety officer will:

- Lead the online safety committee
- Keep up to date with the latest risks to children whilst using technology; familiarise him/ herself with the latest research and available resources for school and home use.

- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing this policy regularly along with other related document and bring any matters to the attention of the Head teacher.
- Advise the Head teacher, governing body on all online safety matters.
- Meets with the online safety governor regularly meets regularly to discuss current issues, review incident logs and filtering / change control logs
- Provides training and advice for staff and ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Retain responsibility for the online safety incident log, ensure staff know what to report and ensure the appropriate audit trail as well as a log of incidents to inform future online safety developments. **SEE APPENDIX A**
- Engage with parents and the school community on online safety matters at school and/or home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure any technical online safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the LA and ICT technical support.
- Make him/ herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function, liaise with the Head teacher and responsible governor to decide on what reports may be appropriate for viewing.
- Reports regularly to the Senior Leadership Team and in partnership with them decides on the investigation/ action and sanctions process for any online safety incidents.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
  - Anti-virus is fit for purpose, up to date and applied to all capable devices.
  - Windows (or other operating systems) updates are regularly monitored and devices updated as appropriate.
  - Any online safety technical solutions such as internet filtering are operating correctly.
  - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and the Head teacher.
  - Passwords may not be applied to shared pupil areas. Passwords for staff will be a minimum of 8 characters.
  - The IT system administrator password is to be changed on a bi-monthly basis.
  - Machines are encrypted and memory sticks containing pupil information are encrypted.
- The school meets required online safety technical requirements and any Local Authority / other relevant body Online safety Policy / Guidance that may apply.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet/ email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and/ or Online safety Lead for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school / academy policies

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the head teacher or online safety officer.

- They have an up to date awareness of online safety matters and the current school policy and practices.
- They have read, understood, signed and abide by the acceptable use policy **SEE APPENDIX B**
- All digital communication with pupils and parents/ carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities and implement current policies with regard to the use of digital technologies, mobile devices, cameras etc in lessons.
- Pupils understand and follow the online safety and acceptable use policies and have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Any online safety incident is to be reported to the online safety lead, and/ or the head teacher and recorded in an online safety incident log.
- The reporting flowcharts contained within this online safety policy are to be understood.

Senior Designated Person for Safeguarding:

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

Online safety Group

The Online safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

Members of the Online safety Group will assist the Online safety lead with (where relevant):

- the production / review / monitoring of the school online safety policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool
- the educating and sharing of good practise with the whole school community

Parents and Carers

Parents play the most important role in the development of their children; as such the school will offer the parents the skills and knowledge they need to ensure online safety of children outside the school environment. Through parent's evenings, school newsletters, regular promotion and links on our website, the school will keep parents up-to-date with new and emerging online safety risks and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student acceptable use policy to show support of the policies and procedures before any access can be granted to school ICT equipment or services. **SEE APPENDIX C** They will also sign a parent's AUP policy at the start of each school year. **SEE APPENDIX D**

Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. **SEE APPENDIX E**

Education - All 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. 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 / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- 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 pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The boundaries of use of the ICT equipment and services in this school are given in the student acceptable use policy; **(APPENDIX C)** any deviation or misuse of ICT equipment or services will be dealt with in accordance to the behaviour policy.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers education sessions
- High profile events and campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications through the school website and termly online safety newsletters

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff 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 Online safety Lead 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 meetings and training days.
- The Online safety Lead will provide advice / guidance / training to individuals as required.

Training – Governors

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

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

Technology

The Avenue Infant School uses a range of devices including Ipads, Cameras, PCs and Laptops. The school will be responsible for ensuring that the school network is as safe and secure as reasonable 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.

In order to safeguard the student and in order to prevent loss of personal data we employ the following:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- Technology and services will be risk assessed to reduce the potential of harm to children and young people when using technology introduced by the school. **APPENDIX F**
- There will be regular reviews and audits of the safety and security of school academy technical systems
- All users will have clearly defined access rights to school technical systems and devices

- Servers, wireless systems and cabling are securely located and physical access restricted
- Group and class log ons are used for children in the school as they are age appropriate but the school is aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. To address this, pupils should always be supervised and members of staff should never use a class log on for their own network / internet access.
- Students, visitors and guests will be provided with information on a guest log in and guest wifi access as appropriate.
- The administrator password for the school, used by the IT technical team is also available for the Headteacher and is kept in a locked filing cabinet in the school office. Passwords are also stored securely at Sir Christopher Hatton Academy with the IT technical support team.
- The school Business Manager and IT technical support 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.** We use an educational filtered system that prevents unauthorized access to illegal websites. Illegal content (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. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident; whichever is sooner. The ICT co-ordinator, online safety officer and IT support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the head teacher.
- **Email Filtering:** We use mail filtering software that prevents any infected email to be sent from or received by the school. Infected is defined as: an email that contains a virus or script (i.e malware) that could be damaging or destructive to data; spam email such as a phishing message.
- **Encryption:** All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are to be encrypted. Any loss or theft of device such as laptop or USB drive is to be brought to the attention of the head teacher immediately. The head teacher will liaise with the online safety governor to ascertain whether a report needs to be made to the Information Commissioner's Office.
- **Passwords:** All staff will be unable to access a device that can access personal or confidential data without a unique username and password. The ICT co-ordinator and IT support are responsible for ensuring that these are kept secure.
- **Anti – Virus:** All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT support will be responsible for ensuring this task is carried out and will report to the head teacher if there are any concerns. All USB peripherals will be scanned before use.
- Senior Leaders 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. Senior Leaders monitor attempts to access blocked sites and act accordingly.
- 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.
- Guests such as trainee teachers, supply teachers or visitors will be given the 'guest' login to use the school systems. They will have signed an acceptable use policy before using the school IT systems.
- An agreed policy is in place through the signing of a staff AUP (**APPENDIX D)** regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.

Safe Use

Internet: Use of the internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this online safety and the staff acceptable use policy; pupils (or their parents) upon signing and returning their acceptance of the acceptable use policy.

Email: All staff are reminded that their emails are subject to Freedom of Information Requests, and as such the email service is to be used for professional work based emails only. Emails of a personal nature are not permitted. Similarly use of personal emails for work purposes are not permitted.

Incidents: Any online safety incident is to be brought to the immediate attention of the head teacher and online safety officer. The online safety officer will assist you in taking the appropriate action to deal with the incident and fill out an incident log e.g. any threatening or inappropriate pop-ups/pages will be reported to the online safety officer and this will be addressed.

Use of digital and video images (in conjunction with the Camera and Image Policy)

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:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- 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 pupils are published on the school website (covered as part of the AUP signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Policy APPENDIX D
- Pupil's work can only be published with the permission of the pupil and/ or parents or carers.

Data Protection (in conjunction with the School Personal Data Handling Policy)

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 will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing (Appendix of the Data Protection Policy) which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

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

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

<u>Communications</u>

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students / pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school / academy 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 digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. 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 must be in place.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / 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 should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and online safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

The school policy restricts usage as follows:

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

On-line gaming (educational)	X				
On-line gaming (non educational)		X			
On-line gambling		X			
On-line shopping / commerce	X				
File sharing	X				
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting eg Youtube		X			

Responding to incidents of misuse

PREVENT

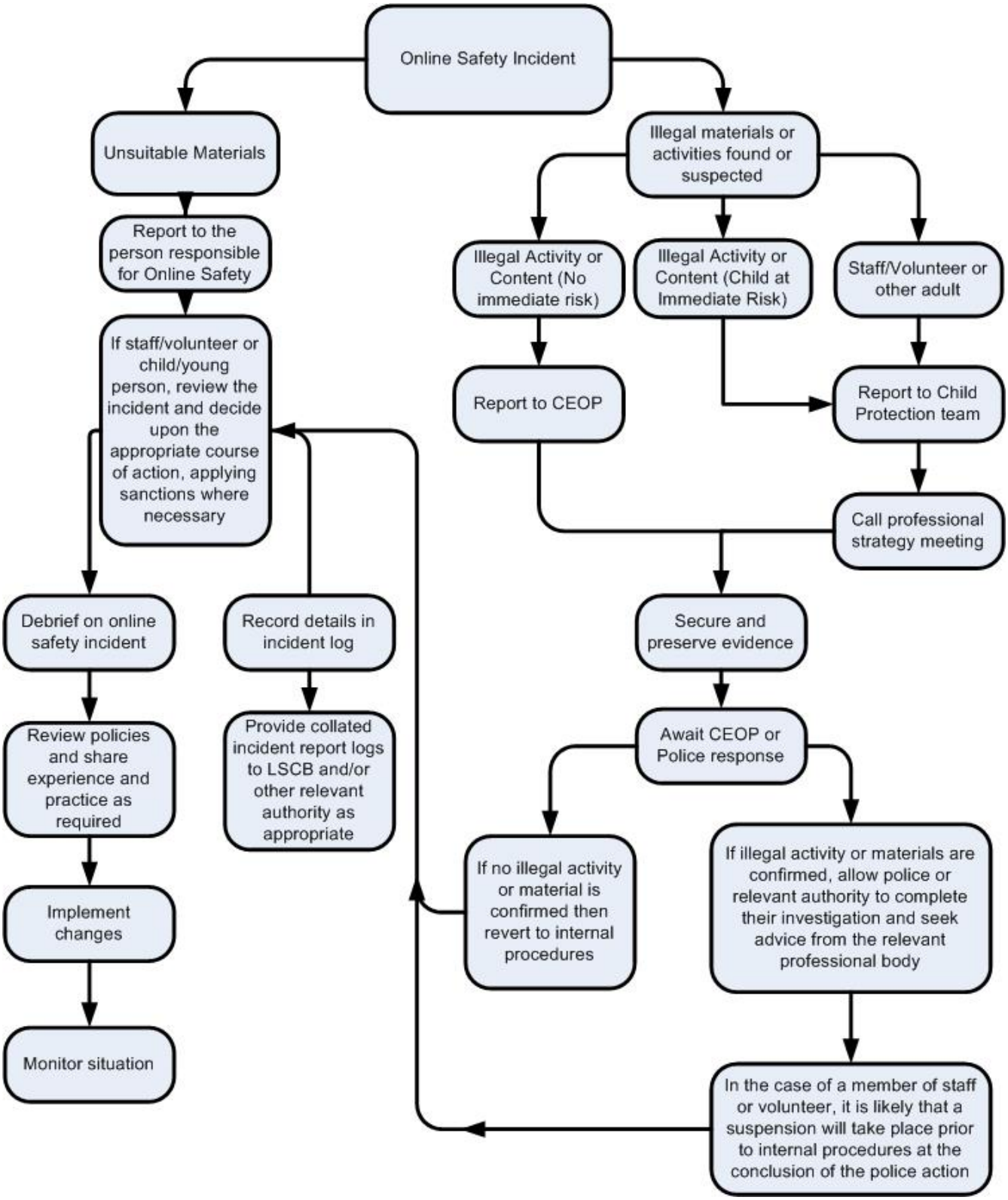
In accordance with the Prevent Strategy, which aims to prevent children and young people being exposed to extremist views and at risk of radicalisation, staff are all trained on the channel programme http://course.ncalt.com/Channel_General_Awareness/01/index.html

This responsibility extends to online safety and protecting children from extremist material online. Through this training, staff are aware of how the internet is used to radicalise people. Filtering should prevent access to such extremist sites but any material accessed at school should be treated as an online safety incident and dealt with accordingly. Disclosures or concerns regarding exposure outside of school should be treated as a safeguarding incident and dealt with in accordance with the Safeguarding policy and procedures (cf. Safeguarding policy).

Parents and carers are informed about the risks of radicalisation and extremism via online safety newsletters and The Prevent Action Plan which is available the school website.

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. The ICT misuse policy (**APPENDIX G)** will be used to guide processes alongside the flowchart below.

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

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

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in conjunction with the school's behaviour and or/ disciplinary policy.

Head Teacher Name: **Helen Morrall** Signed:

Chair of Governors: **Mark Ryan** Signed:

Reviewed: **May 2017** Next Review: **May 2018**

APPENDIX A – Online safety Incident Log

The Avenue Infant School The Avenue, Wellingborough, Northants, NN8 4ET 01933 276366	THE AVENUE INFANT SCHOOL **Online safety Incident Log**	The Avenue Infant School The Avenue, Wellingborough, Northants, NN8 4ET 01933 276366

Online safety Lead Teacher Online safety Lead Governor	Helen Morrall Mark Ryan	
Details of Online safety Incident		
Type of incident	Bullying or harassment	
	Online bullying or harassment	
	Sexting (self-taken indecent images)	
	Deliberately bypassing security or access	
	Hacking or virus propagation	
	Racist, sexist, homophobic, religious hate material	
	Terrorist material	
	Sexual images/ pornography	
	Other (Please specify) ……	
Date of Incident		
Time of Incident		
Where the incident occurred		
Name of person reporting the incident		
Who was involved in the incident	Child/ young person	
	Staff member	
	Other (Please specify)	

Description of the incident		
Nature of the incident	Accidental	
	Deliberate	
Did the incident involve material being…	Created	
	Viewed	
	Printed	
	Shown to others	
	Transmitted to others	
	Distributed	

Could this incident be considered as…	Harassment	
	Grooming	
	Cyberbullying	
	Sexting (self taken indecent imagery)	
	Breach of acceptable use policy	
	Other (please specify) ……	
Action Taken	Staff	
	Incident reported to head/ senior leader	
	Child involved (if necessary)	
	Parents informed	
	Disciplinary action taken (please specify)	
	Child debriefed	
	Senior leader/ Online safety Lead	
	Advice sought from children's social care	
	Incident reported to police	
	Incident reported to CEOP	
	Incident reported to Internet Watch Foundation	
	Incident reported to IT services	
	Online safety policy to be reviewed/ amended	

Outcome of incident/ investigation

Children's Social Care		
Police/ CEOP		
School		
Individual staff member/ child		
Parents		
Other (HR/ Legal etc)		

Learning from the case

Key Learning Point 1	
Key Learning Point 2	
Key Learning Point 3	

Recommendations and Timescales

Recommendation 1		Timescale to be implemented	
Recommendation 2		Timescale to be implemented	
Recommendation 3		Timescale to be implemented	

Appendix B – Staff Acceptable Use Policy

THE AVENUE INFANT SCHOOL

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the Online Safety Policy. Once you have read and understood both you must sign this policy sheet.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupil's learning and will, in return, expect staff and volunteers 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. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. This includes not allowing anyone else at home to use school ICT systems without agreement from the headteacher.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers **using official school systems**. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school or profession into disrepute.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school

- When I use my mobile devices (laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not deliberately upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not deliberately use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. Any inadvertent breach of this will be reported to the Online safety Lead.
- 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos).
- **Social networking** is allowed in school in accordance with the online safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

I understand that I am responsible for my actions in and out of the *school:*

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

APPENDIX C

Please share this with your child and ask them to sign at the bottom/ sign for them to show that they understand and will follow these rules.

THE AVENUE INFANT SCHOOL

Acceptable Use Policy – Pupils

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school equipment for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences to my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date :

APPENDIX D

THE AVENUE INFANT SCHOOL

Parent / Carer Acceptable Use Agreement

Name of Child **Class**

Digital technologies have become important 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 children will be responsible users and stay safe while using the internet and other communications 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 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.

We will try to ensure that children will have good access to digital technologies to enhance their learning and will, in return, expect the children to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents are aware of the school expectations of the children in their care and children will need to sign/ adults sign on their behalf to indicate that they are aware of the school rules for safe internet and technology use. Parents are requested to sign the permission form below at different points to show their support of the school in this important aspect of the school's work.

INTERNET USE

PLEASE NOTE: The school's ICT system & virus protection are updated and reviewed regularly. Pupil's computers are on a different network to the school's administration system. A high level filtering system is in operation on the school's network which only allows access to websites suitable for primary aged children.

RULES FOR RESPONSIBLE INTERNET USE

★ When children are accessing the internet they will be supervised by an adult.
★ Pupils will not be issued with individual email accounts (until Year 2 when separate permission will be sought) but may have opportunity to use a group/class email address under direct supervision.
★ Pupils will only visit websites that an adult has given them permission to do so.
★ Pupils will be advised that if they see anything that they are unhappy with, they will tell an adult immediately.

1. I have read and understood the school rules for responsible internet use and give permission for my child to access the internet.
2. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.
3. I agree that the school cannot be held responsible for the nature or content of materials accessed through the Internet and mobile technologies.
4. I agree that the school is not liable for any damages arising from use of the Internet facilities where all reasonable precautions have been taken.
5. I will discuss the school's acceptable use policy for children with my child and I will encourage my child to adopt safe use of the internet and digital technologies at home. I will inform the school if I have concerns over my child's online safety.

I give permission for my child to access the internet whilst in school.

Signed

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

*How do we show **common courtesy** online?*

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

*How do we show **common decency** online?*

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

*How do we show **common sense** online?*

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

I agree to follow the guidelines for use of social media as outlined above and understand that there will be appropriate action taken by the school should any inappropriate behaviour which impacts upon the school or any member of the school community be drawn to their attention.

Signed

In order to support those parents who may be less familiar with use of the internet we have listed a variety of additional measures that you could take at home to support your child's safe use of the internet in the 'online safety' part of our school website. You can also find our online safety questionnaire and policy on there.

Alternatively, speak to your child's class teacher or Mrs Morrall our online safety lead, about any support that you would like or suggestions that you might have.

APPENDIX E

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use personal devices that I've brought into school for activities that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will 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 download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name _____ Signed _____

Date _____

APPENDIX F

RISK LOG

(Examples given are only examples – not specific to the school)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	online safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	

Likelihood: How likely is it that the risk could happen (foreseeability).
Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE:
1 – 3 = Low Risk
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body. Final decision rests with Headteacher and Governing Body.

Risk Assessment

Risk No.	Risk
3	In certain circumstances, students will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well being of the child.
LIkelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3
Impact 3	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.

Risk Assessment	HIGH (9)
Risk Owner/s	online safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using XXXXXXXX software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The online safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school online safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.

Approved / Not Approved (circle as appropriate) **Date:**

Signed (Headteacher) : **Signed (Governor) :**

APPENDIX G

The ICT Misuse Policy

1. Aim

The ICT (Information and Communication Technology) Misuse Policy aims to ensure that any allegation, which is made in respect of intentional or unintentional misuse of any online technologies, is addressed in a responsible and calm manner. This includes any known or suspected breaches of the acceptable use policy, camera and image policy, internet policy and mobile phone policy.

Allegations must be dealt with promptly, sensitively and fairly in line with agreed procedures. The ICT misuse policy should also outline the sanctions that are applied if an incident occurs.

The overall priority should be to ensure the safety and wellbeing of children and young people at all times. If it is suspected at any stage that a child or young person may have been or is considered to be subject to abuse, the safeguarding policy and procedures should be implemented with immediate effect. These procedures should also be followed if an allegation of abuse is made against any employee, manager, volunteer or student. The safeguarding policy should take precedence over all others and referrals should be made to the appropriate agency as deemed necessary.

2. Scope

The ICT misuse policy applies to all individuals who have access to and/or are users of work related ICT systems. This includes children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.

The policy should be implemented in respect of any potential breaches of the acceptable use policy, camera and image policy, internet policy and mobile phone policy.

3. Responsibilities

The registered person and the senior designated person for safeguarding are responsible for ensuring that the procedures outlined in this policy are followed. These procedures should be followed if an allegation of misuse is made against a child, young person or adult.

4. Policy Statement

Clear and well-publicised policies and procedures which will influence practice are the simplest and most effective way for the safe use of ICT to be upheld. Such policies and procedure should ensure the promotion of acceptable use and clearly define those behaviours which are not. The sanctions to be imposed in respect of any incidents of misuse should be identified.

It is important that:

- Relevant online safety policies and procedures are fully implemented, monitored and reviewed. These policies and procedures should be rigorous, manageable and reflective of practice and should be shared with all ICT users. The senior designated person for safeguarding is responsible for the management of such policies.

- All ICT users should be made aware of possible signs of potential misuse. Adults, in particular, are responsible for observing practice and behaviours, so that any significant changes in such are identified at the earliest opportunity.
- All ICT users should be made aware that the misuse of ICT and/or breaches of relevant policies and procedures are taken seriously, and that potential sanctions could be applied, should such concerns be raised.
- Effective reporting and whistle-blowing procedures should be in place and promoted.

It should be acknowledged, however, that no system or procedure can be considered completely safe, secure and fool-proof. It should therefore be accepted that the potential for ICT to be misused, whether intentionally or unintentionally will remain. The aim of the online safety policies is therefore to minimise such opportunities and risk.

5. Procedures

General

All incidents should be dealt with on an individual case by case basis, and an escalating tariff of agreed sanctions put in place.

The context, intention and impact of each incident should determine the response and actions to be taken. This allows a degree of flexibility in the application of sanctions. For example, a series of minor incidents by one individual is likely to be treated differently than a one-off occurrence; similarly unintentional and intentional access to inappropriate websites will instigate different levels of intervention and sanctions.

All online safety incidents should be recorded and monitored, and any potential patterns in behaviours identified, to enable such issues to be addressed proactively and for protection to be afforded.

All incidents

The following procedure should be followed for all incidents.

- The incident should be reported to the senior designated person for safeguarding. A written incident record should be made, and the situation monitored.
- The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident may be escalated to a 'serious' level.
- If the incident relates to the inadvertent access to an inappropriate website, it should be added to the banned or restricted list and filters should be applied, where relevant.
- In respect of misuse by children and young people, parents and carers must be informed of the alleged incident and should be advised of any actions to be taken as a result.
- Sanctions should be applied in accordance with the acceptable use policy.

There will always be the possibility that through access to the internet children and young people may gain unintentional access to inappropriate materials. Such material may not be illegal, but is unsuitable in a childcare environment and should be acted on.

Reporting

An open reporting policy should be in place which means that all inadvertent breaches and access to inappropriate materials are reported. The non-reporting of such breaches should result in the concern being escalated.

Serious Incidents

All serious incidents must be dealt with promptly and reported to the senior designated person for safeguarding and the registered person immediately.

The context, intention and impact of the alleged misuse must be considered.

Appropriate actions should be agreed between the senior designated person for safeguarding and the registered person. All details should be accurately and legibly recorded. The reason why any decision is made should also be noted.

If at any stage a child or young person is or has been subject to abuse of any form, the safeguarding policy should be implemented with immediate effect. A referral should be made through Northamptonshire County Council protection procedures or through children's social care and the police, where applicable.

If the incident relates to an allegation made against an employee, manager, volunteer or student; and there is a suggestion that a child or young person has been subject to any form of abuse, the safeguarding policy will again be implemented with immediate effect. The local authority designated officer must be contacted in the first instance in respect of any allegation made against an adult. The police and Ofsted must also be contacted.

No internal investigation or interviews should be carried out in respect of any allegations, unless explicitly requested otherwise by an investigating agency.

If allegations of abuse are made, children's social care, the police and/or the Local Authority designated officer will be the investigative bodies. It must therefore be ensured that no action is taken which could compromise any such investigations.

Where applicable, any hardware implicated in any potential investigations of misuse should be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers and portable media technology.

Internal disciplinary procedures should not be undertaken until investigations by the relevant agencies have been completed. Legal or human resources advice should be sought prior to carrying out any internal investigations and/or instigating high-level disciplinary procedures.

On completion of both internal and external investigations, or sooner where appropriate, an online safety review should be undertaken and policies and procedures amended and updated as necessary. A consultation on any proposed revisions should be held with all ICT users as appropriate. Revised policies and procedures should be circulated as applicable.

By nature, serious incidents most often involve illegal materials and activities, including the viewing, possession, taking, making and distribution of indecent images; bullying or harassment through the use of

portable media devices such as mobile phones, or grooming. These incidents may be instigated by a child, young person or adult.

The following incidents must always be reported to the police, SWCPP, childrens social care, Local authority designated officer and Ofsted.

- Discovery of indecent images of children and young people.
- Behaviour considered to be 'grooming'.
- Sending of obscene materials.

By not reporting such incidents, an offence may be committed.

The seriousness of such allegations should be fully recognised, and all such incidents must be reported to the police immediately. No attempt should be made to download, print or send any materials found. Further offences could be committed by doing so.

If potentially illegal material is discovered, as far as is reasonable practical, the equipment or materials found should not be touched. Computers or other devices should not be switched off unless authorised to do so by the police. The focus must be on preventing further access to the illegal content by keeping other individuals out of the immediate area. Where necessary the monitor should be turned off (but the computer remains on).

6. Illegal material and activities which must be reported to the Internet Watch Foundation

A report should also be made to the Internet Watch Foundation – http://www.iwf.org.uk/reporting.htm
If potentially illegal materials, including images of child abuse have been accessed online, giving details of the website address. If it is unclear whether the content is illegal or not, the concern should be reported as a matter of caution.

7. Media attention

If a serious incident occurs, it may attract intense media interest and speculation. On such occasions, every possible attempt should be made to ensure that children and young people, parents and carers are protected and supported appropriately.

An agreed media strategy should be implemented, and statements only released by authorised personnel, in accordance with information sharing procedures. In all instances, the prime concern should be the safeguarding and welfare of the children, young people and their families. Advice should be taken from services for children and young people where appropriate before any media engagement is undertaken.

8. Authorisation and review

Agreed by:……..

Authorised signatory:……

Date:……..

Date of review:……