APPENDIX 6 - ONLINE SAFETY FAQS

How will the policy be introduced to Pupils?

- Rules for Internet access will be posted in all rooms where computers are used;
- Pupils will be informed that Internet use will be monitored;
- Instruction in responsible and safe use should precede Internet access;
- A module on responsible Internet use will be included in the PSHE programme covering both home and school use;
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up;
- Pupils will be made aware of the acceptable use of technology and sign upon enrolment.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security;
- Security strategies will be discussed at staff meetings;
- Virus protection will be installed and updated regularly;
- Personal data sent over the Internet will be encrypted or otherwise secured;
- Use of portable media such as USB sticks, SD Cards and Hard Drives to carry work should be kept confidential by staff and not used in public computers;
- Files held on the school network will be regularly checked;
- All network system and administration passwords are to be recorded by the IT Department and kept in a secure place with regular updates.

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the 'responsible Internet Use' statement included in the school handbook before using any Internet resource in school;
- All new staff will be taken through the key parts of this policy as part of their induction;
- All staff including teachers, learning support assistants and support staff will be provided with the school Online Safety Policy and have its importance explained as part of the child protection training requirement;
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user;
- Staff development in safe and responsible Internet use, and on the school Internet Policy will be provided as required;
- Breaching this online safety policy may result in disciplinary action being taken and access to ICT being restricted or removed;
- Staff will read and sign *Staff Code of Conduct for ICT*- prior to using school ICT equipment in the school;
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a member of the Senior Leadership Team
- Complaints of Internet misuse will be dealt with by the Headmaster;
- Any complaint about staff misuse must be referred to the Headmaster;
- Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Children-Child Protection Policy and procedures;
- Pupils and parents will be informed of the complaint procedure;
- Parents and Pupils will need to work in partnership with staff to resolve issues;
- As with drug issues, there may be occasions when the Police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the responsible Internet Use Policy in newsletters, the parent portal and on the school website;
- Internet issues will be handled sensitively to inform parents without undue alarm;
- A partnership approach will be encouraged with parents and could include information booklets, practical sessions and suggestions for safe Internet use at home;
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Why is the use of Internet and ICT important? Not only is familiarity with the use of ICT equipment a core requirement, but the efficient use of the equipment and available resources is also considered key – for example, the use of email for efficient

communication and the correct use of the Internet for research. Staff across the school are making increased use of ICT, which benefits not only the quality of teaching and support services but also their professional development. It is equally important that staff are properly equipped and supported to make the most efficient use of ICT resources. In particular, ICT is extremely beneficial in engaging our pupils, who have learning and physical disabilities. It can also help them to access parts of the curriculum, which they might not otherwise be able to engage with.

All pupils deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" ICT facilities including online resources and services. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The school has a duty to provide pupils with quality Internet access as part of their learning experience. In order for the school to maintain such an environment for learners (pupils and adults) everybody must be aware of the need to ensure on-line protection (online safety) and subsequently understand the principles of this policy and the expectations of school practice as documented below.

How is the Safe Use of ICT and the Internet Promoted? The school takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community. Our School has in place an Internet firewall, Internet content filtering and antivirus software, and various IT security policies, which help to ameliorate the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe and we will further promote safe use of ICT and the Internet by educating pupils and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly. The school will ensure that the use of Internet derived materials by staff and Pupils complies with copyright law. We help pupils to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our PSHEE and SMSC provision. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferInternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)

How does the Internet and use of ICT benefit education in our school?

- Pupils learn effective ways to use ICT and the Internet including safe and responsible use;
- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils worldwide;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support;
- Exchange of curriculum and administration data with LA and DfE;
- Support of the wider curriculum through the use of word processing, spreadsheet and presentation tools, specialist applications, and the use of the Internet for research purposes.

How will Pupils learn to evaluate Internet content?

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval;
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use;
- If staff or Pupils discover unsuitable sites, the URL (address) and content must be reported immediately to the teacher, who will inform the Online safety Officer and IT Department;
- Staff and Pupils should ensure that their use of Internet derived materials complies with copyright law;
- Pupils should be taught to be critically aware of the materials they read and show how to validate information before accepting its accuracy;
- Pupils will be taught to acknowledge the source of information used and to respect copyright.

How is Filtering Managed? Having Internet access enables pupils to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. All unsuitable websites will be filtered and automatically blocked by our security system (Smoothwall) and will not be made accessible to pupils. In addition, pupils' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert our DSL. The IT Department will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of pupils. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some pupils may find ways to

access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at we believe that the benefits to pupils having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of minors along with the school share the responsibility for setting and conveying the standards that pupils should follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide pupils towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio etc.

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect pupils are reviewed and improved;
- If staff or pupils come across unsuitable on-line materials, they must report it to the Online safety Officer and ICT Coordinator immediately;
- The school will take every step to ensure that appropriate filtering systems are in place to protect pupils from unsuitable material and the methods used will be reviewed regularly;
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk).

How are Emerging Technologies Managed? ICT in the 21st Century has an all-encompassing role within the lives of pupils and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by pupils may include:

- The Internet
- E-mail
- Instant messaging
- Social media
- Blogs
- Podcasts
- Video streaming sites
- Chat Rooms
- Online Games/Sites
- Music streaming apps/sites
- Mobile phones with camera and video functionality;
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

How to React to Misuse by Pupils and Young People:

Step 1: Should it be considered that a child or young person has deliberately misused ICT, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.

Step 2: If there are to be further incidents of misuse, the child or young person will be suspended from using the Internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with a senior Lead and the most appropriate course of action will be agreed.

Step 3: The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding Children-Child Protection Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

How is Printing Managed? As well as being a significant capital cost, the consumables (ink, laser printer toner and drums, and paper) associated with printing represent one of the most expensive ongoing costs associated with ICT. Whilst the school would not wish to discourage the proper use of printers, it is important to ensure that printing facilities are used efficiently and effectively. Pupils and staff are asked to take care not to waste printing resources, for example by using "Print Preview" to check work before sending it to the

printer and by using colour print only when necessary.

What are the categories of Cyber-Bullying? Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to pupils or young people, or posting inappropriate material in a public digital locale;
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where pupils and young people are sent unpleasant messages as they conduct real-time conversations online;
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying

General Housekeeping: The ICT equipment used by the school represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order. In addition, the ICT resource is finite e.g. computers can run out of disk space; users should be encouraged to think about the amount of file storage they use and the need to keep it well organised. The school does not currently operate a quota system for disk space or mailboxes, but will consider doing so should the need arise.

The following will apply:

- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy;
- Normal school rules and consideration of others applies;
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

What are the Pupil Rules?

- Do not use ICT without permission;
- Food and drink must not be consumed near any computer equipment anywhere in the school
- Do not move about the room while seated on a chair;
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement;
- Computer faults should be promptly reported to the ICT Co-ordinator. Please do not attempt to repair them yourself;
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at the workstation.

<u>At the end of a session</u>:

- Log off/shut down according to instructions;
- Replace laptops as directed;
- Wind up and put away any headsets.

What has Research into Cyber Bullying Found? Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyber-bullying is done by pupils in the same class or year group and although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

- Between a fifth and a quarter of pupils have been cyber-bullied at least once over the previous few months;
- Phone calls, text messages and email are the most common forms of cyber-bullying;
- There is more cyber-bullying outside school than in;
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone;
- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying;
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying;

- Website and text bullying are equated in impact to other forms of bullying;
- Around a third of those being cyber-bullied tell no one about the bullying.

What is the impact on a child of ICT based sexual abuse?

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

How do I stay secure on the Internet?

- Do not type any personal details (including your name or email address) into a web site unless you are absolutely sure of the authenticity and trustworthiness of the associated company;
- The use of chat rooms is prohibited;
- The use of Instant Messaging is prohibited;
- The use of Internet-based email or newsgroups is prohibited except with the prior written approval of the Head.

Why is Promoting Safe Use of ICT Important?

Our School takes very seriously the importance of teaching pupils (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community.

What does the school's Mobile Phone Policy Include?

- The commitment to keep the pupils safe;
- How we manage the use of mobile phones, taking into consideration staff, pupils on placement, volunteers, other professionals, visitors and parents/carers;
- How we inform parents/carers, visitors and other professional of our procedures;
- What type of mobile phones will be used on educational visits and learning outside the classroom;
- The consequences of any breaches of this policy;
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

Technology and Prevent Duty: As part of an integrated policy linked to the Prevent strategy, the school also has a duty to ensure that pupils are prevented and protected from the risk of being radicalised through the access to extremist propaganda, e.g. from ISIL. The school must promote British values through the curriculum and SMSC and SRE. Teachers must also be aware of their responsibility to monitor and report any serious concerns they have about a pupil's use or access to inappropriate material, especially that which undermines British values and tolerance of others. The school's network and facilities must NOT be used for the following activities:

- Accessing or downloading pornographic material
- Gambling
- Accessing sites or social media channels that promote extreme viewpoints and radical propaganda
- Gambling
- Soliciting for personal gain/profit
- Revealing or sharing proprietary or confidential material
- Representing personal opinions about the school
- Posting indecent or humiliating images or remarks/proposals

We ensure pupils are safe from terrorist and extremist material when accessing the Internet in school, including by ensuring suitable filtering is in place. The DfE advises that Internet safety will usually be integral to the ICT curriculum and can also be embedded in PSHEE, for example. Every teacher needs to be aware of the risks posed by online activity of extremist and terrorist groups. For further information, please refer to our *'Preventing Extremism and Radicalisation'* Policy.

Prevent – Top ten FAQs

We are receiving a number of queries to the support@isi.net inbox concerning inspection expectations in relation to the *Prevent* strategy so it may be useful if we address the most frequently asked issues.

1. Where can we learn more about *Prevent*?

There are two key source documents for the *Prevent* strategy:
Statutory guidance (Home Office) – see paras 1-27 generally and 57-76 for sector specific guidance for schools Advice for schools (Department for Education).

2. What do we have to do?

The over-arching legal duty is to **"have due regard to the need to prevent people from being drawn into terrorism"** and, in so doing, have regard to guidance issued by the Secretary of State.

In summary, the national statutory guidance from the Home Office, and sector specific advice from the Department for Education places the following expectations on schools:

Demonstrate effective leadership: display an awareness and understanding of the risk of radicalisation in your area and institution; communicate and promote the importance of the *Prevent* duty to staff; ensure staff implement the *Prevent* duty effectively.

Train staff: ensure staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism; ensure staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism and are shared by terrorist groups; ensure staff know where and how to refer pupils and young people for further help.

Work in partnership with other agencies: co-operate productively, in particular, with local *Prevent* co-ordinators, the Police and local authorities, and existing multi-agency forums, for example Community Safety Partnerships; ensure that safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Children's Partnership (LSCP).

Share information appropriately: ensure information is shared between organisations to ensure, for example, that people at risk of radicalisation receive appropriate support.

Risk assess: assess the risk of pupils being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. This should be based on an understanding, shared with partners, of the potential risk in the local area or your school's particular circumstances. This means being able to demonstrate both a general understanding of the risks affecting pupils and young people in the area and a specific understanding of how to identify pupils who may be at risk and what to do to support them.

Build resilience to radicalisation: promote fundamental British values through the curriculum and through social, moral, spiritual and cultural education; equip pupils with knowledge, skills and understanding to prepare them to play a full and active part in society; ensure your school is a safe place to discuss sensitive issues, while securing balanced presentation of views and avoiding political indoctrination.

Safeguard and promote the welfare of pupils: put in place robust safeguarding policies to identify pupils at risk, and intervene as appropriate by making referrals as necessary to Channel or Children's Social Care, for example.

Ensure suitability of visiting speakers: operate clear protocols for ensuring that any visiting speakers, whether invited by staff or by pupils themselves, are suitable and appropriately supervised.

IT policies: ensure pupils are safe from terrorist and extremist material when accessing the Internet in school, including by ensuring suitable filtering is in place. The DfE advises that Internet safety will usually be integral to the ICT curriculum and can also be embedded in PSHEE, for example. Every teacher needs to be aware of the risks posed by online activity of extremist and terrorist groups.

It is for schools to use their own judgement to fill in operational detail about how best to implement the duty in the context of the level of risk in their locality as advised by their Local Safeguarding Children Board (LSCB) or other local agencies and the assessed risks to their own pupils. The role of inspectors is to raise awareness of the duty and consider whether the measures schools have in place appear effective in each school's particular context. In particular, inspectors will check that schools know how to respond to pupils who may be targeted or influenced to participate in radicalism or terrorism.

Do we have to have a separate *Prevent* policy? The Prevent duties can largely be implemented through schools' existing safeguarding duties using, for example, current reporting lines and training processes. It is not a requirement to create a separate dedicated *Prevent* Policy. However, the Home Office statutory guidance introduces a new requirement that policies "set out clear protocols for ensuring

that any visiting speakers – whether invited by staff or by pupils themselves – are suitable and appropriately supervised. This protocol can be a standalone document or be part of another policy or document.

What IT filtering systems must we have? No technical guidance has been prescribed concerning the levels of filtering, which are to be considered appropriate. This means that schools have discretion as to how they approach this aspect of the prevent duty. Inspectors will assess and challenge on the basis of whether what is in place appears effective in practice to ensure pupils are kept safe from terrorist and extremist material when accessing the Internet in school. Keeping safe on-line is as much about educating pupils to think critically and about appropriate behaviour on-line as technical solutions.

What is the definition of a visiting speaker? There is no definition of a visiting speaker. Schools should exercise their own reasonable judgement to determine who is a visiting speaker.

Do we have to check all our visiting speakers? Schools must ensure all visiting speakers are suitable. There is scope for local discretion as to how. For example, a school could choose to check all speakers or to check all those whom risk assessment indicates warrant closer attention. The over-arching strategy should be recorded in the written protocol mentioned in 3 above.
When it comes to inspection, the burden is on the school to demonstrate to inspectors how they meet the duty. Inspectors will expect verbal assurances from schools to be backed up by documentary and other evidence that protocols are put into practice on the ground.

What checks must we run on visiting speakers? The means by which schools ensure the suitability of their speakers are not prescribed (except in the event that they happen to come within any of the usual categories in the Independent school Standards and Keeping Children Safe in Education, such as “staff”). schools need not confine their approach to the usual formal checks; Internet searches, for example, may sometimes be more instructive than formal vetting checks.
This is compatible with KCSIE which advocates in para. 43 that "... governing bodies and proprietors should prevent people who pose a risk of harm from working with pupils by adhering to statutory responsibilities to check staff who work with pupils, taking proportionate decisions on whether to ask for any checks beyond what is required; and ensuring volunteers are appropriately supervised". © Independent schools Inspectorate 2015.

What do we have to record in our Single Central Register about visiting speakers? The formal recording requirement for the SCR have not changed. Schools must decide which, if any, formal checks are required and must be recorded in the SCR by reference to the usual considerations such as role, frequency, supervision, payment (as not all visiting speakers are volunteers), whether speakers are employed by another organisation.

Paras 277 and 278 of the ISI Regulatory Handbook, September 2015, do not create new SCR recording duties but remind schools to join up their thinking about *Prevent* duties and with vetting duties because, as set out above, the Part 4 checks are now no longer the last word in suitability checks when it comes to visiting speakers.
Some visiting speakers are volunteers. Para. 73 (last line) of KCSIE notes: "Where checks are carried out on volunteers, schools should record this on the single central record." However, this is a recommendation; it is not a requirement to record checks on volunteers the SCR where a secure alternative approach is used instead. Inspectors will be looking to see whether schools have thought through their chosen approach, whether they are implementing their protocol rigorously and whether it is effective.

What training must we have? As a minimum, schools should ensure that the Designated Safeguarding Lead undertakes Prevent awareness training and is able to provide advice and support to other members of staff on protecting pupils from the risk of radicalisation. Schools should consider and arrange further training in the light of their assessment of risks.

What are the potential legal consequences if we do not take the *Prevent* duty seriously? Where the Secretary of State is satisfied that a school has failed to discharge the duty under the Prevent strategy to have regard to the need to prevent people from being drawn into terrorism, the Secretary of State may give directions to the school to enforce performance of the duty. A direction can be enforced by court order.

What are the rules for publishing content online?

- Staff or Pupil personal contact information will not be published on the school website. The only contact details given on our website will be the school address and telephone number;
- Pupil’s full names will not be used anywhere on the school website or other on-line space;
- We may use photographs of pupils or their work when communicating with parents and the wider community, in newsletters and in the school prospectus;

- Photographs will be checked to ensure that they are suitable (photos of pupils in swimwear would be unsuitable).