Policy No: 11.1

APPLEFORD SCHOOL

E-SAFETY POLICY INCLUSIVE CYBER BULLYING, ACCEPTABLE USE AND SOCIAL MEDIA

This policy applies to the whole school, including boarding

The Policy is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office. All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours including activities away from school.

Monitoring and Review: This policy is subject to continuous monitoring, refinement and audit by Dr Peter Gardner (Managing Director), the Advisory Board and Mr David King (Headmaster). The Proprietor (Board of Directors) will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. This discussion will be formally documented in writing. The Proprietor recognises the expertise staff build by undertaking safeguarding training and managing safeguarding concerns. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the update/reviewed policy and it is made available to them in either a hard copy or electronically.

Signed: Dated: September 2019

P. Gardner D. King

Dr Peter Gardner, Managing Director Mr David King, Headmaster

This policy will be reviewed no later than September 2020, or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.

Introduction: The primary purpose of this Policy is to safeguard pupils and staff Appleford School. It details the actions and behaviour required from pupils and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements we have a whole school approach to e-safety. Our key message to keep pupils and young people safe is to be promoted and should be applied to both online and offline behaviours. Within our E-Safety Policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding Children-Child Protection Policy (please refer to our Safeguarding Children-Child Protection Policy cited in related documents). Also see related documents to this E-safety Policy.

This policy informs and supports a number of other school policies, including our Safeguarding Children-Child Protection Policy and our Preventing Extremism and Radicalisation Policy. The staff and pupil Acceptable Use Policies (AUPs) are central to the E-safety Policy and should be consulted alongside this policy. The E-safety Policy will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies. The Pupil Council will be consulted regarding any changes to the Pupil AUP and the Staff body regarding any changes to the Staff AUP. All staff should read these policies in conjunction with the E-Safety Policy. This is particularly important with regard to the Prevent

Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Safeguarding Children-Child Protection and Preventing Extremism and Radicalisation Policies.

Roles and Responsibilities: Our nominated E-Safety Officer is Iona Gray, who has responsibility for ensuring online safety will be considered an integral part of everyday safeguarding practice. This role overlaps with that of the Designated Safeguarding Lead (DSL) role and in all matters regarding safeguarding and E-safety.
The role will include ensuring:

- Young people know how to use the Internet responsibly and that parents and teachers have the right measures in place to keep pupils safe from exploitation or radicalisation.
- Pupils are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- To ensure that pupils use ICT safely and securely and are aware of both external and peer to peer risks when using ICT including cyberbullying and other forms of abuse.
- All staff, volunteers and the board will receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- The Acceptable Use Policy (AUP) is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be transparent and updated as agreed in school policies.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- An appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- A current record of all staff and Pupils who are granted access to school ICT system is maintained.

Staff/Volunteers Use of IT Systems:
Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the 'Staff Code of Conduct for ICT) (please see appendices) before using any school ICT resource. In addition:

- All staff will receive annual update e-safety training.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password protected computers and other devices Staff are advised to follow the "How do I stay secure on the Internet?" section in the E-Safety FAQ document.
- In lessons where Internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- Occasionally pupils may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study. Every request to do so, should be auditable with clear reasons for the need.
- The Internet can be used actively to gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved web browsers and email systems which have appropriate security in place. Additionally files should not be saved directly from the Internet unless they can be scanned for viruses etc first.
- Additionally, staff should not communicate with pupils through electronic methods such as social networking sites, blogging, chat rooms, texts or private email. Instead, only the school email system should be used.
- Education material made by and for classes and uploaded to password protected youtube channel, i.e. videos of lessons, activities or fieldtrips, must be logged for record keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the school's E-Safety Officer.
2. The E-Safety Officer should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanction will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the CEOP or the police will be informed.
5. No pupil or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

Teaching and Learning: Internet use is part of the curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. E-safety is a focus in all areas of the curriculum and key e-safety messages are reinforced regularly, teaching pupils about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour.

Staff should be vigilant in lessons where pupils use the Internet. If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with school policy. Staff will be provided with sufficient e-safety training to protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements

The school's Internet access is designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use. Access levels reflect the curriculum requirements and age of pupils. Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of on-line materials is a part of teaching/learning in every subject.

Pupils Use of IT Systems: All pupils must agree to the IT Acceptable Use Policy before accessing the school systems. Pupils at Appleford School will be given supervised access to our computing facilities and will be provided with access to filtered Internet (see FAQ Document) and other services operating at the school. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and

development needs of pupils and young people. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Appleford School will 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 Personal, Social, Health and Economic Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. 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)
- The UK Safer Internet Centre (www.saferinternet.org.uk)

Communicating and Educating Parents/Guardians in Online Safety: Parents will be provided with a copy of the IT User Acceptance Policy, and parents will be asked to sign it, as well as pupils age eight and older. Appleford School recognises the crucial role that parents play in the protection of their pupils with regards to online safety. The school organises annually an awareness session for parents with regards to e-safety which looks at emerging technologies and the latest ways to safeguard pupils from inappropriate content. The school will also provide parents and carers with information through newsletters, web site and the parent portals. Parents and guardians are always welcome to discuss their concerns on e-Safety with the school, who can direct them to the support of our E-Safety Officer if required. Parents and carers will be encouraged to support the school in promoting good e-safety practice.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school recognises that if required, data may need to be obtained by relevant parties such as the Police.

Radicalisation and the Use of Social Media to Encourage Extremism: The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people;
- Confirming extreme beliefs;.
- Accessing likeminded people where they are not able to do this off-line, creating an online community;.
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Appleford School has a number of measures in place to help prevent the use of social media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils.
- Pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*

Reporting of E-Safety Issues and Concerns Including Concerns Regarding Radicalisation: Appleford School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding e-safety should be made to the E-safety Officer who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the e-

safety officer. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding Children-Child Protection Policy.

Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting pupils from the risk of on-line radicalisation. Appleford School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We 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. Staff safeguard and promote the welfare of pupils and know where and how to refer pupils and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Emerging technologies, such as mobile phones with Internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.
- We will audit ICT use to establish if the E-Safety Policy is sufficiently robust and that the implementation of the E-Safety Policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Heads of Departments will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered *wifi* access.
- Appleford School takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard pupils from potentially harmful and inappropriate material on-line without unreasonable "over-blocking" (para 67, 69 and new Annex C of KCSIE 2016).
- Appleford School recognises that pupils may choose to circumvent certain safety precautions by using devices over 3G and 4G. To help provide a safe environment for all pupils, we will supplement the systems filtering with behaviour management and additional staff/pupil training.

Mobile Electronic Devices (Phones, Laptops, Ipads and Tablets; please see appendix 4 for more details)

Mobile telephones are permitted both in boarding houses and in academic school buildings. During the school day phones are only to be used by pupils during break time and lunch time by pupils in Yr 10 and above, unless in the boarding houses. Appleford School pupils (all ages) are only allowed to have mobile phones in school with advance permission from parents, which is included in the parent acceptable use policy – this permission will be sought prior to the start of each school year - and these are kept on site at the risk of the individual pupil. If in the rare case a pupil brings a mobile phone into lessons without signed consent or permission from the teacher, this must be handed over to the class teacher who will hand the device to the School Office. Upper School pupils must ensure that their devices are kept in a secure place, e.g. their school bag or in their pocket. Appleford School is not responsible for any devices lost by pupils. (See Safeguarding Children-Child Protection policy).

Cyber-Bullying: is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Cyberbullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt

with under the school's child protection procedures (see our Safeguarding Children-Child Protection Policy).
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;
- **Chat room bullying and online grooming** involve sending menacing or upsetting responses to pupils or young people when they are in a web-based chat room;
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where pupils and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, GroupMe, Skype, Facebook Messenger, Snapchat, GoogleHangouts etc.) as they conduct real-time conversations online;
- **Bullying via websites and social networks (an example of this would be Facebook, Twitter, Instagram, etc.)** 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.

Pupils should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

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. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

There are no circumstances that will justify adults possessing indecent images of pupils. Adults who access and possess links to such websites will be viewed as a significant and potential threat to pupils. Accessing, making and

storing indecent images of pupils is illegal. This will lead to criminal investigation and the individual being barred from working with pupils, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with pupils. Adults should ensure that pupils are not exposed to any inappropriate images or web links. Where indecent images of pupils or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Chat Room Grooming and Offline Abuse: Our staff will need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child. Specific focus and attention should be made with regard to gaming activities as these are known to be associated with grooming through seemingly innocent contacts.

Taking and Storing Images of Pupils Including Mobile Phones (See our related documents including Appendix 5): Appleford School provides an environment in which pupils, parents and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined in appendix 5 of this policy. This prevents staff from being distracted from their work with pupils and ensures the safeguarding of pupils from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a Mobile Phone Policy (which includes:

- The commitment to keep the pupils safe.
- How we manage the use of mobile phones at Appleford School taking into consideration staff, pupils on placement, volunteers, other professionals, trustees, 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.

For further information relating to E-safety procedures, refer to the E-Safety Frequently Asked Questions (FAQ) in Appendix 4. It covers the following topics on the relevant page as follows:

1 How will the policy be introduced to pupils? How will staff be consulted and made aware of this policy? How will complaints regarding Internet use be handled? How will parents' support be enlisted?

2 Why is the use of Internet and ICT important? How is the safe use of ICT and the Internet promoted? How does the Internet and use of ICT benefit education in our school? How will pupils learn to evaluate Internet content?

3 How is filtering managed? How is emerging technologies managed? How to react to misuse by pupils and young people
4 How is printing managed? What are the categories of Cyber-Bullying? General Housekeeping what are the pupil rules?
5 What has research into Cyber Bullying found? What is the impact on a child of ICT based sexual abuse? What is the impact on a child of ICT based sexual abuse? How do I stay secure on the Internet? Why is promoting safe use of ICT important? What does the school's Mobile Phone Policy Include?
6 Where can we learn more about Prevent? What do we have to do?
7 Do we have to have a separate *Prevent* Policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?
8 What training must we have? What are the potential legal consequences if we do not take the *Prevent* duty seriously? What are the rules for publishing content online?

Related documents:

- E-Safety Appendices 1-6
- Safeguarding Children- Child Protection Policy; Anti-Bullying Policy; Behaviour and Discipline Policy.
- Prevent Duty: Tackling Extremism and Radicalisation Policy, Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE); The School Rules.
- Acceptable use of ICT Sign off forms for Staff/Pupils; Use of Photographs Sign-off Form.
- What to do if you are worried; www.thinkyouknow.co.uk.

Legal Status:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Pupils Safe in EDUCATION* (KCSIE) *Information for all schools and colleges* (DfE: September 2016) incorporates the additional statutory guidance, *Disqualification under the Childcare Act 2006* (February 2015) and also refers to non-statutory advice for teachers, *What to do if you're worried a child is being abused* (HM Government: March 2015)
- *Working Together to Safeguard Pupils* (WT) (HM Government: 2015) which also refers to non-statutory advice, *Information sharing* HM Government: March 2015); *Prevent Duty Guidance: for England and Wales* (March 2015) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for schools and childminders (June 2015)* and *The use of social media for on-line radicalisation (July 2015) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE)*
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'
- Prepared with reference to DfE Guidance (2014) *Preventing and Tackling Bullying: Advice for school leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in schools.*
- Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*
- The Data Protection Act 1998; BECTA and CEOP.

Student acceptable use policy

I will not post anything (including language or pictures) which might upset or offend other people.

I will make sure all my passwords are safe and will not share them with anyone else. I understand I must not use or share anyone else's login details or use a device someone else is logged on to.
I will change my password straight away if somebody else knows it /finds out what it is.
I will make sure I log out after every network session.

I will only go on appropriate material. I will not visit websites that might be inappropriate or illegal. I know that the school can see what I'm looking at on the internet. If I see anything that I shouldn't accidentally, I will tell an adult straight away, this could be other people's information or illegal / inappropriate websites. Offensive things include abuse, racist, terrorist, sexist, homophobic, bullying, porn or illegal.

I will not give or put any of my own or anyone else's personal details on social media. I know that email is not always private. Any messages or communication through the internet that supports illegal activities will be reported to the police.

I will be careful when I download anything. I know that the illegal download/copyright is not allowed and would be reported to the police. I will not download any software, system utilities or resources from the internet without adult permission.

I will turn off mobile hot spots. I will not harm, destroy or remove equipment. I will not harm, destroy or remove other people's work or website that is connected to the system.

I know that my device and any activity on it is my responsibility. I know that the school has the right to take away and look at my device.

All pupils must follow the rules outlined in this policy when using school ICT resources and equipment, including all Internet access and the Virtual Learning Environment (VLE), accessed from both in and outside of school, and on school provided or personal electronic devices. Breaking these conditions may lead to: confiscation of any electronic devices, close monitoring of the pupil's network activity, investigation of the pupil's past network activity, withdrawal of the pupil's access and, in some cases, permanent removal from the School and even criminal prosecution. Pupils are also expected to take care of school-issued electronic devices and any damage to them may result in fines to replace or fix damaged devices. Misuse of the Internet will be dealt with in accordance with the school's Behaviour and Discipline Policy and, where there is a safeguarding risk, the Safeguarding Children-Child Protection Policy. The school is not responsible for any loss of data on the network, computers connected to the network or data storage used on the network (including USB memory sticks). Data held on the network will be backed up for a limited period. Pupils are responsible for backups of any other data held. Use of any information obtained via the network is at the pupil's own risk.

Pupil access to networked resources is a privilege, not a right. Pupils will be expected to use the resources for the educational purposes for which they are provided.

Pupils are expected to use the network systems in a responsible manner. It is not possible to compile a complete set of rules about what is, and what is not, acceptable; however, the above should be a guide and in cases of dispute the decision of the Head of School will be final.

Pupil agreement:

I agree to follow the school rules on the use of school network resources and mobile electronic devices. I will use the network and all mobile electronic devices in a responsible way and observe all of the conditions explained in both the E-Safety Policy and this Acceptable Use Policy. I understand and accept the consequences of breaking these rules.

Print pupil name……

Pupil Signature……Date…….

Parent/Guardian agreement:

I understand that my child has agreed to accept the terms of the E-safety and Pupil AUP Policy and I confirm that I accept the terms of the agreement. I also allow my child to bring his/her personal electronic devices and understand that the pupil is responsible for its safekeeping and appropriate usage while in transit to and from and at school.

I have read and understood the E-Safety Policy.

Print Parent/Guardian name……..

Parent/Guardian Signature…… Date…….

Appendix 12– Staff and Directors Acceptable Use Policy

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the School's E-Safety Policy and for further information and clarification. You must not use any ICT on-site until you have signed this Code of Conduct document and logged it with HR.

- I will respect all ICT equipment/facilities at Appleford School and will report any faults that I find or any damage that I accidentally cause to the school's e-safety Lead (IT Manager).
- I agree to abide by this policy in respect of any of my own ICT equipment or mobile devices that I bring on site. If any ICT device (personal or School-issued) is being used inappropriately or illegally on site, this will result in disciplinary action.
- I understand that no photographs of students or their personal data may be taken with or stored on my personal electronic devices, including personal computers.
- I will not allow unauthorised individuals to access school email, Internet, the school network /other School systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the School's network and data security and confidentiality protocols, deleting data securely which is no longer necessary.
- I will only use the approved, secure email system(s) for any School business.
- I will only use the approved School email or other School approved communication systems with pupils or parents/carers, and only communicate with them on appropriate School business.
- Photos of students will not be uploaded to personal social media accounts.
- I am familiar with the School's Data Protection Policy and I agree I am responsible for the security of all personal data in my possession. I agree that any personal data that relates to an identifiable person is kept locally on the school's secure servers and will not be taken off site unless absolutely necessary. If data is taken off site, a removable memory device will be used which is encrypted or contained within password-protected files to prevent unauthorised access.
- I agree and accept that any iPad, computer or laptop loaned to me by the School, is provided to support my professional responsibilities. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow School data security protocols when using any such data at any location.
- I am responsible for my use of my own log-in details and if I suspect that my log-in details have become known to others, or I suspect a data breach, then I will immediately report this to the data protection officer who is the Bursar, Charles Njoko. (See Data breach policy for further details).
- I agree that my use of Appleford School ICT equipment/facilities will be monitored for safeguarding purposes. I understand that the results of such monitoring and recording may be shared with other parties if I break the terms of this Acceptable Use Policy.
- I will not deliberately attempt to access any unsuitable websites, services, files or other resources when on-site or using Appleford School equipment/facilities. I understand that I may temporarily access blocked websites, services and other online resources using only tools that are provided by Appleford School. I agree that I will not display blocked websites, services and other resources to others until I have fully assessed the materials and have found them to be entirely suitable for the intended audience.
- I agree that the provision of Appleford School ICT equipment/facilities including the email and Internet system are for educational purposes, although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other clauses in this document.
- I am aware that downloading copyright materials, including music and video files without paying the appropriate licence fee is often a criminal act. I am aware that any involvement in criminal acts relating to the use of ICT on-site or using Appleford School equipment/facilities may result in disciplinary or legal action. I will not deliberately engage in these acts.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the School's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not deliberately view, send, upload or download any material that is unsuitable for the School environment whilst I am in that environment or using any ICT equipment/facilities belonging to Appleford School. If I accidentally encounter any such material then I will immediately close, but not delete in the case of emails, the material and immediately report it to the E-Safety Officer, (Iona Gray), or to a senior member of staff. I will not be penalised if I view unsuitable material accidentally and by reporting such incidents I will help to improve e-safety. If I am in any doubt about the suitability of any material, or if a colleague raises any doubts, then I will not (re)access the material without the agreement of the E-Safety Officer. I will not access any material that the E-Safety Officer has rated as unsuitable.

- Unless specifically authorised to do so, I will not disclose any of my personal details, other than those that identify me professionally, nor log any such details on websites whilst using Appleford School equipment or facilities. If I disclose any additional personal details contrary to this instruction, then I agree that these details can be recorded and that I will not hold Appleford School responsible for maintaining the security of the details I have disclosed.
- I agree that professional standards of communication will be maintained at all times. I recognise that staff should not communicate with students through personal electronic devices or methods such as social networking sites, blogging, chat rooms, text messaging, messenger applications or private email. Instead, only the School email system may be used.
- I will use a school mobile phone to contact parents and pupils as necessary on school outings or when offsite with pupils.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the School's most recent Online-Safety policies.

I agree to abide by all the points above.

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

Signature .....…… Date .....

Full Name ..... (printed)

Job title ……

APPENDIX 3

USE OF MOBILE TECHNOLOGY INCLUDING TAKING AND STORING IMAGES OF PUPILS POLICY

Applies to:

- The whole school, out of school care, the after school clubs and all other activities provided by the school, inclusive of those outside of the normal school hours.
- All staff (teaching and support staff), pupils on placement, the proprietor and volunteers working in the school.

Related documents:

- Safeguarding Children-Child Protection Policy 17.1
- E-Safety Policy including ICT Acceptable Use Policy 11.1

Availability:

This policy is made available to parents, staff and pupils in the following ways: via the School website, parent portal and on request, a copy may be obtained from the Office.

Monitoring and review: This policy is subject to continuous monitoring, refinement and audit by David King (Headmaster). The Managing Director will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. This discussion will be formally documented in writing. The Managing director recognises the expertise staff build by undertaking safeguarding training and managing safeguarding concerns. As such, staff have the opportunity to contribute to and shape our safeguarding arrangements and child protection policy. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the update/reviewed policy and it is

Signed: Date: September 2019

Dr Peter Gardner	Mr David King
Managing Director	Headmaster

This policy was last reviewed and agreed by the Managing Director of the school in September 2019 and will next be reviewed no later than September 2020 or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Introduction

Whilst we welcome the use of mobile phones and cameras for educational purposes and the convenience they offer and recognise that learning to use digital technology is an important part of the ICT and wider curriculum, equally we have to ensure the safeguarding needs of the pupils are met and staff, parents and volunteers are not distracted from their care of pupils. Mobile phones, alongside other technologies aim to change the way we communicate. This speed of communication will often provide security and reassurance; however, as with any other form of technology there are to be associated risks. Pupils and young people must be encouraged to understand such risks to enable them to develop the appropriate strategies, which will keep them safe.

As with online safety issues generally, risks to pupils and young people should be broadly categorised under the headings of:

• Content
• Contact
• Conduct
• Commerce.

These issues are to be managed by reducing availability, restricting access and increasing resilience.

This philosophy is to be applied to the use of mobile phones through the Mobile Phone Policy. Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation

that the personal use of mobile phones is to be limited to specific times and uses as to be agreed with the Designated Safeguarding Lead. Safe and secure storage facilities are to be made available to store personal belongings as necessary.

Aims: The aim of the Mobile Phone Policy is to protect pupils and young people from harm, by ensuring the appropriate management and use of mobile phones by all individuals who work or visit our school. Pupils and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way; and to be alert to the potential risks of such use. This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

Scope: The Mobile Phone Policy will apply to all individuals who are to have access to and or be users of personal and/ or work-related mobile phones within the broadest context of the setting environment. This will include pupils and young people, parents and carers, volunteers, pupils, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

Policy statement: It is to be recognised that it is the enhanced functions of many mobile phones that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and cyberbullying. It must be understood that should mobile phones be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to pupils and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

Code of conduct: A code of conduct is to be promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the pupils and young people in their care. It is to be ensured that all teachers and their co-ordinators will:

- Be aware of the need to protect pupils from harm.
- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Be vigilant and alert to potential warning signs of misuse.
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to potential allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Be responsible for the self-moderation of their own behaviours.
- Be aware of the importance of reporting concerns immediately.

It is to be recognised that studies consistently indicate that imposing rigid regulations and/or 'bans' on the actions of others are counterproductive and should be avoided. Such imposition will lead to a culture of suspicion, uncertainty and secrecy. An agreement of trust is therefore to be promoted regarding the carrying and use of mobile phones within the school. This is to be agreed by all service users, including all pupils, young people and adults who are to come into contact with the school setting.

Storage and Review of Images: Images of pupils are stored securely. Digital photographs and videos are reviewed annually and are deleted when no longer required. We regularly check and update our web site, when expired material is deleted.

Appleford School Website: Photographs and videos may only be uploaded to the school's website with the Headmaster's approval. Pupil's surnames are never used on our website. When pupils join Appleford School, we

ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld such photographs/videos are not published of the individual child concerned. Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

External Photographers: Professional photographs are taken throughout the year at school shows, by local media and Professional School Portraits. The Headmaster ensures that professional photographers are DBS checked and that they have their own stringent regulations, which ensure safeguarding of pupils from inappropriate use of images.

Appropriate use of a Mobile Phone During the School Day (Including Social Networking): Mobile phones have a place on outings or in school buildings, which do not have access to a school landline. In these cases, they are often the only means of contact available and can be helpful in ensuring pupils are kept safe. Ideally staff should use school mobile phones in these circumstances but, if required to use a personal phone, should input 141 to ensure their own number is hidden.

By arrangement with SLT, a member of staff's mobile phone may be designated as the means of communication for specific activities. The leader of the trip should ensure all participants (including parents, volunteers and partners) in the activity are aware of this Mobile Phone and Camera Policy.

When leaving the school building with pupils (e.g. for sport, or on school trips), the mobile phones of all members of staff must be switched on and turned to loud to ensure that staff can be contacted by the school. Contact numbers for all members of staff accompanying the pupils must be left at Reception and a list of contact telephone numbers for all pupils should be with the leader of the off-site activity (although these must be kept confidential). Group leaders will also be provided with a school-issued mobile phone.

Staff must not post anything onto social networking sites such as Facebook that could be construed to have any impact on the organisation's reputation. (We advise all our staff to carefully restrict their Facebook profiles to ensure they cannot be contacted by parents and pupils, this could involve removing their last name from their page). We explain to staff that although they are able to accept friendship requests from friends who may also be parents of pupils at the school, staff must be aware of the potential issues this could cause. Staff must not post anything onto social networking sites that would offend any other member of staff or parent using the setting. If any of the above points are found to be happening, then the member of staff involved will face disciplinary action, which could result in dismissal. We also advise faculty and staff not to accept friend requests from pupils until graduates have been out of school for three years.

Pupils and Mobile Phones: The school takes precautions to ensure that pupils limit access to their personal mobile devices during the school day, and reserves the right to confiscate and monitor personal devices when deemed necessary for safeguarding concerns. In school, pupil's mobile phones should be turned off and should remain in Reception during the school day. Pupils in Yr 10 and above should keep their mobile devices switched off and kept securely in on their person or in their school bag unless permission has been given by the classroom teacher for example: note taking or data collection. In the event of a mobile phone being used in a lesson without permission from the teacher, the phone should be confiscated and given to the Head of Pastoral Care.

In the boarding houses, mobile phones are permitted during free time, although their use is prohibited after lights out. Phones can be collected from younger pupils (up to Year 10) and this provision can be extended to pupils who persistently use their phones at inappropriate times. Mobile devices must not be used to directly take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission. Pupils and staff are informed about the statutory framework regarding the sharing and publishing of photographs and videos, regardless of the media chosen. Staff must adhere to the Safeguarding Children-Child Protection Policy and Staff Behaviour Policy (Code of Conduct).

Any use of mobile technology to intimidate, bully, harass, threaten or attempt to radicalise others or breach copyright laws will be counted as an infringement of network use and breach of discipline and will be dealt with in

accordance with the school's Behaviour and Discipline Policies. This may result in disconnection from the network, confiscation of the mobile technology and/or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission and if in doing so, School and statutory guidelines are not breached.

Pupils are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

The School has the right to confiscate and search any mobile electronic device (personal or school-issued) if it suspects that a pupil or staff member is in danger or has misused a device. This will be done in accordance with the School's policy on searching and confiscation as set out in the Behaviour and Discipline Policy.

Use of images: displays etc

We will only use images of our pupils for the following purposes:

- Internal displays (including clips of moving images) on digital and conventional notice boards within School premises.
- Communications with Appleford School community (parents, pupils, staff), for example newsletters.
- Marketing Appleford School both digitally by website, by prospectus [which includes a DVD and Youtube channel], by displays at educational fairs and other marketing functions [both inside the UK and overseas] and by other means.

Images that we use in displays and on our web site: The images that we use for displays and communications purposes never identify an individual pupil. Instead, they name the event, the term and year that the photograph was taken (for example, 'Sports Day, Summer Term 2016'). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc. in their proper context. We never use any image that might embarrass or humiliate a pupil. Pupils are always properly supervised when professional photographers visit Appleford School. Parents are given the opportunity to purchase copies of these photographs.

The pupils take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents present often take photographs of these memorable events, which may include groups of pupils. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents.

Media coverage: We will always aim to notify parents in advance when we expect the press to attend an event in which our pupils are participating, and will make every effort to ensure that images including pupils whose parents or guardians have refused permission for such images of their pupils to be used are not used. We will always complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the pupils of celebrities.

Staff induction: All new teaching and office staff are given guidance on the school's policy on taking, using and storing images of pupils.

Use of Mobile Phones for Volunteers and Visitors: Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in school. The exception to this would be at an organised event. Staff should remind parents regularly of school policy with regard to mobile phone use with the following statement on weekly emails, when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g. a family album) and so are exempt from the Data Protection Act 1998. Please be aware these images (which may include other pupils) must not be shared on social

networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of the Act." If they wish to make or take an emergency call they may use the office and the school phone.

Parental use of mobile phones/cameras within the school buildings: The growth of hand-held mobile technology and interconnectivity has implications for the safety of pupils, so in order to reflect the policy on safeguarding and child protection, it is essential parents do not use their mobile phones/cameras in the school building, apart from circumstances as outlined below. Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of pupils or in public areas of the school such as during meetings and school events.

The school records images of pupils, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of pupils while performing and disturbance within the audience.

Other mobile technology: *At Appleford School, we recognise the value of mobile technology within our curriculum and our pupils' accommodation. From Yr 10 and above pupils may bring their own devices to school to support their studies. Any personal device that pupils bring to the school must be used appropriately in line with the Pupils' Acceptable Use Policy and must be kept securely. Where a pupil is found to be misusing a school or personal device, or accessing inappropriate content, the device may be confiscated by the school and appropriate action taken. When accessing the school WiFi, staff and pupils must adhere to their ICT acceptable use Policy. Staff, pupils, volunteers and parents are responsible for their own mobile devices and the school is not responsible for theft, loss, or damage.*

Driving and the law: The use of hand-held phones while driving, whether to make or receive a call, is prohibited. The only exception to this will be in the event of a genuine emergency call to 999 or 112, if it would be unsafe for the driver to stop. Hand-held mobile phones used with an earphone and microphone are covered under the ban, as they still require the user to hold the phone to press buttons or to read a message on the phone's screen.

The Proprietor and employees of the school will not require any employee to receive or make calls on a mobile phone while driving. Mobile phones must instead be directed to the message/voicemail service while driving.

The Headmaster will not assist in the payment of any fine levied against anyone using a hand-held mobile phone while driving. An employee will be regarded as driving if the engine is running, even if the vehicle is stationery. Notification of any contravention of these requirements may be regarded as a disciplinary matter.

Appendix 4

E-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 faculty 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 e-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 e-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.
- We will maintain a list of e-safety resources for parents.
- Parents will be invited to attend an e-safety workshop annually.

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

(e-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?

Appleford 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. Appleford 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 Appleford School 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. Appleford School will 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 E-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 it's 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 systems 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 IT Department. 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 Appleford School 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 Appleford 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 E-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 (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Social media
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com / http://www.facebook.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com,http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'Internet ready'.
- 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 manager 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?

Appleford 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 at Appleford School taking into consideration staff, pupils on placement, volunteers, other professionals, trustees, 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.

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 Board (LSCB).

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).

Appendix 5 – Parents, volunteers and visitors photographing pupils

Appleford School provides an environment in which pupils, parents and staff are safe from images being recorded and inappropriately used. The growth of hand-held mobile technology and interconnectivity has implications for the safety of pupils, so in order to reflect the policy on safeguarding and child protection, upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined below. This includes where pupils are on school trips or residential. Neither are volunteers or visitors are permitted to take photographs or recordings of the pupils. Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of pupils. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in school.

Parental use of mobile phones/cameras whilst on the school grounds
Appleford School allows parents to take photos of their own children at organised events such as a school performance, sporting event or celebration of learning. We will remind audiences of this at the start of each event, where practicable. Staff will also remind parents regularly of school policy with regard to mobile phone use with the following statement when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g. a family album) and so are exempt from the Data Protection Act 1998. Please be aware these images (which may include other pupils) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of the Act." If parents wish to make or take an emergency call whilst on school grounds, they may use the office and the school phone.

Parents are welcome to take photographs of their own pupils taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events. Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts. We always print a reminder in the programme of events where issues of copyright apply. Additionally, the school records images of pupils, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to

photograph professionally events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of pupils while performing and disturbance within the audience.

When pupils join Appleford School, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld, this must be made clear when the consent form is returned to school so that photographs/videos are not published of the individual child concerned. The pupils take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents are welcome to take photographs of these memorable events, which may include groups of pupils. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents. Wherever possible, parents who take photographs of groups of children who are in the care of the school should gain consent first, ensuring that once any photographs are taken, they are stored safely and not posted to social media. The school recognises that it cannot police parents taking photographs of pupils who are outside school grounds and not in the school's care, however posting such pictures online may be in breach of the Data Protection Act 1998 without consent of all people within the photograph.

Appleford School

USE OF PHOTOGRAPHS OF PUPILS AND DATA PROTECTION FORM
(To be completed by all new parents)
Photographs
When a pupil is registered at Appleford School, the parent/guardian is asked to complete a 'Registration Form', which includes asking the parent/guardian for permission to use photographs of their child for marketing and publicity purposes including our website, prospectus, adverts, press releases and other marketing literature such as brochures and leaflets. We will not use names next to photographs of pupils on the website (in accordance with the DfE guidelines). This form is in addition to paragraph 6.15 in Appleford School's standard terms and conditions which states "Parents consent to Appleford School making use of information (textual or pictorial) relating to their child whilst they are at Appleford School and after they have left for the purpose of marketing and publicity for Appleford School."