Policy No: 1.6a

APPLEFORD SCHOOL

ONLINE SAFETY AND MOBILE TECHNOLOGY, INCLUSIVE OF CYBER BULLYING, ACCEPTABLE USE AND SOCIAL MEDIA, INCLUDING TAKING AND STORING IMAGES OF CHILDREN POLICY

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.

We have a whole school approach to safeguarding, which is the golden thread that runs throughout every aspect of the school. All our school policies support our approach to safeguarding (child protection). Our fundamental priority is our children and their wellbeing; this is first and foremost.

Legal Status: Complies with The Education (Independent College Standards) (England) Regulations and the National Minimum Standards (NMS) for Residential Special Colleges (RSS) currently in force.

Monitoring and Review: This policy is subject to continuous monitoring, refinement and audit by Dr Peter Gardner (Proprietor and Managing Director), the Advisory Board and Mr David King (Headmaster). The Proprietor 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

Policy Agreed: September 2025
Date Published (including on website): September 2025
Next Review: September 2026

Signed:

P. Gardner

D. King

Dr Peter Gardner
Proprietor and Managing Director

Mr David King
Headmaster and Non-Executive Director

This policy will be reviewed no later than September 2026, or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.

Page Contents

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 online 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 Online 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 Online safety Policy. There are implications with reference to technology and Prevent Duty cited in this policy, as part of an online safety integrated policy linked to the Prevent strategy. However, it is incumbent on Appleford School to also have a free-standing policy regarding the Preventing of Extremism and Radicalisation, which is an essential adjunct to the Online Safety Policy.

Online safety is a running and interrelated theme when devising and implementing our wider school policies and procedures, including our Safeguarding and Child Protection Policy and our Preventing Extremism and Tackling Radicalisation Policy. The staff and pupil Acceptable Use Policies (AUPs) are central to the Online safety Policy and should be consulted alongside this policy. We consider how we can promote online safety whilst developing our curriculum, through our staff training, and also through parental engagement. The Online safety Policy will be reviewed annually by the safeguarding team and Deputy Head 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 Online 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.

Appleford School provides a safe environment for pupils to learn and work in, especially when online. Filtering and monitoring are both important parts of safeguarding pupils from potentially harmful and inappropriate online material. The Headmaster has overall strategic responsibility for filtering and monitoring and works in conjunction with the Designated Safeguarding Lead (DSL) and the IT team, as well as the Proprietor to ensure these standards are met. In accordance with KCSIE (currently in force), the DSL works closely with the members of the senior management team and IT team to ensure that filtering and monitoring is adequate and robust in the school and boarding facility. The DSL and IT team:

- procure and maintain an appropriate system (Smoothwall);
- identify risk issue (age of pupils, Special Education Needs and Disabilities (SEND) issues, English as an Additional Language (EAL), Personal Social Health and Economic Education (PSHEE), Relationship and Sex Education (RSE), County Lines, Bring Your Own Devices (BYOD) etc.);
- carry out regular reviews
- carry out checks as and when required.
- Ensure that the system is robust and blocks harmful content, without unreasonably affecting teaching and learning.
- Ensure that the chosen system is a member of the Internet Watch Foundation (IWF), signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and block access to illegal content including child sexual abuse material (CSAM). The current system is Smoothwall.

All existing school computers and devices are monitored and checked by the IT lead in association with the DSL and senior managers. Boarding pupils are required to register their e-based devices and are recommended to use the school Wi-Fi system.

Roles and responsibilities: Our Head of Safeguarding who is also the DSL, working in conjunction with our IT Lead, is responsible for ensuring the online safety of the school community. Our IT team takes operational responsibility for online safety in the school, but the **lead responsibility** is taken by the DSL, Mrs Julia Hendrickse, for making sure that policy is enforced and that the necessary checks, filters and monitoring are in place. It is the school's responsibility to ensure that pupils are safe from cyber bullying both within and outside the school community and that appropriate steps are taken if an incident occurs. The Leadership Team will also review online

safety and the acceptable use of technology in the school during their regular meetings.

The role includes 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 child to child 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.

Designated Safeguarding Lead (DSL): The Designated Safeguarding Lead (DSL), Mrs Julia Hendrickse, takes **lead responsibility** for online safety in the school. The DSL is a senior member of the management team who has relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is available at all times, for example, a Deputy Designated Safeguarding Lead is also in place should the DSL be absent. In particular, the DSL is responsible for:

- supporting the Proprietor in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- working with the Proprietor, IT Lead and other staff, as necessary, to address any online safety issues or incidents;
- ensuring that any online safety incidents are logged (see appendix 1) and dealt with appropriately inline with this policy;
- ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy**;**
- updating and delivering staff training on online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring (appendix 3 contains a self-audit for staff on online safety training needs);
- communicating any updates regarding online safety to all members of staff;
- liaising with other agencies and/or external services if necessary;
- ensuring all new staff are aware of Appleford's online safety policy during their induction;
- providing regular reports on online safety in the school to the Proprietor. This list is not intended to be exhaustive.

All Staff and volunteers: All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on **acceptable use agreement** (appendix 1)
- Working with the DSL and/or **prevent lead** to ensure that any online safety incidents are logged (seeappendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's **behaviour policy**
- Engage with new safety information and updates, for example at staff meetings or those received via email

This list is not intended to be exhaustive.

Parents: Parents are expected to:

- Notify a member of staff or the Headmaster of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on **acceptable use agreement** of the school's IT systems and internet (appendix 1)
- Engage with our online safety guidance which is regularly shared with parents through our website, newsletters, social media platforms and regular safety briefings via email, raising any concerns that they have.

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

- What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community: Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use agreement (appendix 2).

All Pupils: All pupils will ensure they understand and adhere to our pupil Acceptable Use Policy, which they must sign and return to the DSL. Pupils are reminded of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

Technologies: Hardware and software are developing continuously. The majority of children use online tools to communicate with others locally, nationally and internationally. Access to the internet and other tools that technology provides are invaluable ways of finding, sharing and communicating information. Technology itself is not harmful, but can be used by others to make children vulnerable to abuse.

Breadth of Online Safety Issues: We classify the issues within online safety into **four** areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism;
- **Contact:** being subjected to harmful online interaction with other users; for example: child to child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images; e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams

These issues are to be managed by reducing availability, restricting access, and promoting safe and responsible use.

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

1. Report in confidence to the DSL
2. The DSL 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 about online safety: Our Online Safety Curriculum is closely linked with our Relationships and Sex Education Programme and discusses the links associated with Online abuse and other associated risks. Access levels to ICT reflect the curriculum requirements and age of pupil. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. This teaching is built into existing lessons alongside our wider whole-school approach including visits from external visitors and regular assemblies with a running theme of keeping safe. Pupils will explicitly be taught the following topics through their lessons:

- What Internet use is acceptable and what is not and given clear guidelines for Internet use, including protecting their online identity and privacy;
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications;
- How to evaluate what they see online;
- How to recognise techniques used for persuasion;
- Online behaviour;
- How to identify online risks
- How and when to seek support and report a range of concerns.
- How to recognise and respond to harmful online challenges and online hoaxes.

We recognise that Child-on-Child abuse can occur online and to this end we teach pupils how to spot early warning signs of potential abuse, and what to do if pupils are subject to sexual harassment online. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge.
- 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.

Online Reputation: Online reputation is the opinion others get of a person when they encounter them on-line. It is formed by posts, photos that have been uploaded and comments made by others on people's profiles. It is important that children and staff are aware that anything that is posted could influence their future professional reputation. The majority of organisations and work establishments now check digital footprint before considering applications for positions or places on courses.

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)
- PSHE Association (https://www.pshe-association.org.uk/)
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

The school will therefore seek to provide information and awareness to both pupils and their parents through:

- Acceptable use agreements for children, teachers, parents/carers and governors
- Curriculum activities involving raising awareness around staying safe online
- Information included in letters, newsletters, school website pages
- High profile events/campaigns
- Building awareness around information that is held on relevant websites and/or publications
- Social media policy

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 aged 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 awareness sessions for parents with regards to online 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 online safety with the school, who can direct them to the support of our Online safety Officer if required. Parents and carers will be encouraged to support the school in promoting good online safety practice.

Cyber Security: The school recognises its responsibility to ensure that appropriate security protection procedures are in place to safeguard are systems. As part of our whole-school Online Safety Training, we ensure staff, the Advisory Board and proprietor are updated with the evolving cyber-crime technologies. In addition, the school activity considers the Cyber security standards (DfE: 2025) and uses these as a base for keeping the school and its community safe from cyber-crime**.**

Generative Artificial Intelligence (AI) - Please also see our separate AI Guidance Document: We recognise that generative AI tools, such as Google Bard and ChatGPT, have many uses. These include enhancing teaching and learning, and helping to protect and safeguard pupils. However, it is crucial to consider the risks carried by AI; for example, facilitating abuse in the form of bullying or grooming or exposing pupils to harmful content. This could be in the form of 'deepfakes', where AI is used to create image, audio or video hoaxes that look real. It is important that all staff are aware of the risks posed by AI tools, and that risk assessments are carried out for all new AI tools used by our school. Any use of AI to access harmful content or bully pupils will be treated in line with this policy and our anti-bullying (countering bullying) policy.

We will consider how online safety, including the use of generative artificial intelligence, is reflected as required in all relevant policies and embedded across all areas of the curriculum, included in teacher training and within the role and responsibilities of the designated safeguarding lead as well as discussions with parents. We understand that technology, and risks and harms related to it, evolve, and change rapidly and we will carry out regular reviews of our approach to online safety to consider and reflect the risks to our pupils.

The DfE has published Generative AI: product safety expectations to support schools in using generative AI safely, and explain how filtering and monitoring requirements apply to the use of AI in education.

Characteristics of a strong password

- At least 8 characters – the more characters, the better
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ?]

Note: do not use < or > in your password, as both can cause problems in web browsers.

A strong password is hard to guess, but it should be easy for you to remember – a password that has to be written down is not strong, no matter how many of the above characteristics are employed.

Protecting Personal Data: Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018. The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Pupils are encouraged to keep their personal data private as part of our Online Safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will act responsible for ensuring we have an appropriate level of security protection procedures in place, in order to safeguard systems, staff and learners and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

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:

- Website 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 Online 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 online safety should be made to the Online 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 online 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.

The use of smartphones to access the internet via data is not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed. We recognise the additional risks this has for our pupils in Boarding, who could have unsupervised access to the internet when using their own devices in their free time. To address this, the school works with pupils across our age range to ensure that pupils are educated clearly about the risks of both social media and internet use, alongside regularly monitoring of device usage as appropriate.

- We will audit ICT use to establish if the Online safety Policy is sufficiently robust and that the implementation of the Online 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";
- Appleford School recognises that pupils may choose to circumvent certain safety precautions by using devices over 3G, 4G and 5G. To help provide a safe environment for all pupils, we will supplement the systems filtering with behaviour management and additional staff/parent /pupil training.

Filtering and Monitoring: The school provides a safe environment for pupils to learn and work in, especially when online. Filtering and monitoring are both important parts of safeguarding pupils from potentially harmful and inappropriate online material. The proprietor has overall strategic responsibility for filtering and monitoring. For this to occur, they have assigned a member of senior leadership team (The DSL) and the Advisory Board to be responsible for ensuring these standards are met. The DSL works closely with IT lead and other members of SLT to ensure that filtering and monitoring is adequate and robust in the school and boarding facility. The school considers those who are potentially at greater risk of harm and how often they access the school's IT systems. The school

follows the Filtering and Monitoring Standards (DfE: 2025) which ensures that the school:

- identifies and assigns roles and responsibilities to manage filtering and monitoring systems
- reviews filtering and monitoring provision at least annually
- blocks harmful and inappropriate content without unreasonably impacting teaching and learning (using Smoothwall)
- has effective monitoring strategies in place that meet the school's safeguarding needs

Phishing and Pharming Definition: A phishing email usually contains a link with directions asking the recipient to click on it. Clicking the link transports the email recipient to an authentic looking, albeit fake, web page. The target is asked to input information like a username and password, or even additional financial or personal data. The miscreant that orchestrates the phishing scheme is able to capture this information and use it to further criminal activity, like theft from a financial account and similar types of criminal activity. Pharming is the term used to describe a cyber scam where malicious code redirects a user to a fake website without their knowledge, with the intention of stealing confidential information. As opposed to phishing, pharming requires an attacker to gain unauthorised access to a system. **The school has no intention of changing its financial information, therefore will never accept an email with a link pretending to be the school's accounts department.**

Top tips:

- Never click on hyperlinks in email from an unknown sender, rather manually type the URL into the web browser itself
- Never enter sensitive information in a pop-up window except at those sites that an individual knows to be trustworthy
- Verify HTTPS on the address bar - whenever a person is conveying confidential information online, you must confirm that the address bar reads "HTTPS" and not the standard "HTTP." The "S"confirms that the date is being conveyed through a legitimate, secured channel
- Access personal and financial information only from a computer or device you trust to be free from trojans and keyloggers
- Education on phishing and pharming attacks - staying abreast of phishing scams and the technologyand techniques designed to prevent them is crucial. A plethora of reliable educational resourcesexist on the Internet that are designed to assist a person in preventing phishing attacks
- Report phishing and pharming to the financial institution, the FTC, and the Internet Crime Complaint Center

Mobile and Smart Technology (Phones, Laptops, iPads and Tablets; please see appendix 3 for more details): Mobile telephones are permitted in boarding houses only. During the school day phones are **only** to be used by pupils for monitoring their diabetes. All other pupils must either deposit their mobile device with their Houseparent, or at the school Reception on arrival in the morning. These will be collected upon departure at the end of the school day. Appleford School is not responsible for any devices lost by pupils. (See Safeguarding Children-Child Protection policy).

Cyber-Bullying: Cyber-bullying is defined as 'an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself'. Like other forms of bullying, cyber-bullying is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (please see also the school's behaviour policy.) Cyber-bullying (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, TikTok, Skype, Facebook Messenger, Snapchat, Google Hangouts 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;
- Do something - if you see cyberbullying going on, support the victim and report the bullying.

Cyber-bullying may rise to a level at which it is criminal in character. It is unlawful to disseminate defamatory information via any media, including online. Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

Online Sexual Harassment: Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence. Online sexual harassment includes: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, is unacceptable and will dealt with under our Child Protection Procedures.

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

a. The UK Safer Internet Centre provides an online safety helpline for professionals at **0344 381 4772** and helpline@saferinternet.org.uk. Providing expert advice and support for school staff with regard to online safety issues and when an allegation is received.
b. If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

ICT Based Sexual Abuse (including Sharing nudes/semi-nudes): 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.

Pupils are reminded that 'sharing nudes/semi-nudes' (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 sharing nudes/semi-nudes (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.

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.

Gaming: Online gaming is an activity in which the majority of children and many adults get involved. The school will raise awareness of associated risks:

- By talking to parents and carers about the games their children play and helping them to identify whether they are appropriate
- By supporting parents in identifying the most effective way to safeguard their children by using parental controls and child safety mode
- By talking to parents about setting boundaries and time limits
- By highlighting relevant resources

Social Media, including Facebook, Twitter and Instagram: Facebook, Twitter, Instagram and other forms of social media are increasingly becoming an important part of our daily lives, including part of the school's marketing strategy.

- Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Headmaster for reasons of work
- Staff are advised not to befriend or follow parents of pupils and to keep their personal profile as private as possible
- Staff and pupils are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff and pupils are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff and pupils are aware that their online behaviour should at all times be compatible with UK law. Additionally, more information on best practice for staff can be found in our Staff Behaviour (Code of Conduct) Policy
- Appleford School recognises that Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

Use of Email:

- Whole class/group email addresses may be used at KS2, while pupils at KS3 and above will be provided with individual email addresses for educational use;
- The use of personal email accounts to send and receive personal data or information is prohibited;
- No sensitive personal data shall be sent to any other young persons, staff or third parties via works email;
- Young people are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity;
- Staff members are aware that their email messages may be monitored;
- Any emails sent by young people to external organisations will be overseen by their teacher/support worker and must be authorised before sending;
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Taking and Storing Images of Pupils Including Mobile Phones (See our related documents including Appendix 3): 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 3 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 potential 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, the advisory board, 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.

Remote Learning (Please see our Remote Learning Policy for more details): Where there are periods in which the school is forced to close, yet continue to provide education (such as during the COVID-19 Pandemic) it is important that Appleford School supports staff, pupils and parents to access learning safely, especially considering the safety of our vulnerable pupils. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk.

Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns, and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the Police. Online teaching should follow the same principles as set out in the school's staff and pupils respective Behaviour - Code of Conducts. Additionally, school name will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The school will put additional measures in place to support parents and pupils who are learning from home. This will include specific guidance on which programmes the school is expecting pupils to use and how to access these alongside how pupils and parents can report any concerns that they may have. Guidance will also be issued on which staff members pupils will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our schools Remote Learning Policy. Additionally, the Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, with the day to day responsibility being delegated to the Online Safety Lead who is our DSL. The Headmaster and the DSL are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, which in line with our main safeguarding reporting procedures.

Staff working remotely should wherever possible use their school-issued ICT equipment, however they may use their own computer equipment if this is not practical, as long as it is in accordance with the school's Data Protection Policy. Staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

Related documents:

- Online Safety Appendices 1-6;
- Safeguarding Children - Child Protection Policy; Sexual Violence and Sexual Harassment (Including Child-on-Child Abuse Policy); Anti-Bullying Policy; Behaviour and Discipline Policy; Staff Behaviour (Code of Conduct) 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;
- Mobile and Smart Technology Policy, including taking and storing images of pupils; Acceptable use of ICT Sign off forms for Staff/Pupils; Use of Photographs Sign-off Form.

Legislation and guidance

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent College Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Children Safe in Education* (KCSIE) *Information for all schools and Colleges* (DfE: September 2025) incorporates the additional statutory guidance,
- *Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.*
- *Working Together to Safeguard Children* (WT) (HM Government: December 2023) which also refers to non-statutory advice, *Information sharing* HM Government: March 2015); *Prevent Duty Guidance: for England and Wales* (2023) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for Colleges and childminders (June 2015)* and
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and College staff 'and 'Advice for parents and carers on cyberbullying'
- Prepared with reference to DfE Guidance (2014) *Preventing and Tackling Bullying: Advice for College leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in Colleges.*
- Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*
- The Data Protection Act 1998; GDPR, 2018; BECTA and CEOP.
- Teaching Online Safety in schools (DfE: 2023)
- The policy also takes into account the National Curriculum computing programmes of study.
- Meeting digital and technology standards in schools and Colleges (DfE: 2025) (including Broadband, Cyber-Security and data protection procedures)
- Filtering and monitoring standards for schools and colleges (DfE: 2025)
- Cyber security standards for schools and colleges (DfE: 2025)
- Promoting and supporting mental health and wellbeing in schools and colleges (July 2025)
- Behaviour in schools (February 2024)

Guidance (UK Safer Internet Centre)

- 2023 Appropriate filtering and monitoring definitions published (UK Safer Internet Centre)
- Test Your Internet Filter (UKSIC / SWGfL)
- A Guide for education settings and filtering providers (UKCIS)
- Establishing appropriate levels of filtering (UKSIC)
- Online safety in schools and colleges: questions from the governing board (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people

The following legislation and guidance should be considered:

- Data Protection Act 1998
- Human Rights Act 1998
- Regulatory of Investigatory Power Act 2000
- Computer Misuse Act 1990 – Police and Justice Act 2006
- Prevent Duty – Counter-terrorism and Security Act 2015
- Obscene Publications Act 1959, Protection of children Act 1988, Criminal Justice Act 1988

Pupil 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 Microsoft Teams 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 Headmaster will be final.

Mobile Device
Parent/Guardian Permission

I have read and understand the mobile devices acceptable use policy about appropriate use of mobile devices at Appleford School and I understand that this form will be kept on file at the school and that the details may be used (and shared with a third party, if necessary) to identify a phone should the need arise (e.g. if lost, or if the phone is being used inappropriately).

I give my child permission to carry a mobile device to school and understand that my child will be responsible for ensuring that the mobile device is used appropriately and correctly while under the school's supervision, as outlined in this document.

I understand that the school will not accept any responsibility for loss, damage or theft of a mobile device.

I understand that my child will not be allowed a mobile device in school unless this form has been completed in full, signed and returned.

Name of Parent/carer: (Please print)	
Name of pupil: (Please print)	

Mobile device details:

Make and model number …….

Mobile device telephone number ……

Colour/description of phone ……

Network ……

IMEI number……This can be found by dialling *#06#

I confirm that parental controls are set up on my child's devices with the correct age appropriate content filters.

Android link: Family Link from Google - Family Safety & Parental Control Tools (families.google)

Apple link: Share with your family – Apple Support (UK)

Parent Signature: …… Date: …….

For Boarding pupils
Tick here if you wish your child to have access to his/her phone in boarding. ☐

Pupil Mobile Device Contract for <u>Boarders</u>

- My name must be on my mobile device and I am responsible for looking after my mobile device when in use.
- I am responsible if my mobile device gets lost or broken.
- I will only give my mobile number to my friends and I will never share other peoples' mobile numbers to anyone.
- I will not take photographs/videos/recordings of any pupil or staff at any time.
- If I need to call home during the school day, I will ask reception to contact my parent/carer.
- I will never use my mobile device in the dorms or toilets.
- I will have my device collected before bedtime and kept safe overnight by the Houseparents. The Houseparents will decide when and where mobile devices can be used. This is usually for a set amount of time, in a public space, in the evening after activities.
- The Headmaster or Head of Boarding may search my device if he/she feels it necessary and I understand that if I use my mobile device to look at anything inappropriate, I will have my device confiscated by a member of staff. My parents will be informed and it will not be returned to me until an investigation is concluded.
- I will not <u>upload</u> any data. School work can be shared on Student Shared.
- I understand that using a device to bully or threaten other pupils is not allowed and that 'ganging-up' on anyone, or cyber bulling is not allowed. I will have my mobile device confiscated if I do this.
- I will inform a staff member if I become aware of another pupil using their mobile device inappropriately.
- I agree to these rules.

Print Pupil Name……

Pupil Signature…… Date……

Pupil Mobile Device Schedule for <u>Boarders</u>

- "Mobile Device Parent/Guardian Permission form" **<u>and</u>** "Pupil Mobile Device Contract for Boarders" must be signed before Boarders are allowed to bring in their mobile device.

- Mobile devices must be handed into Houseparents on the morning or evening of arriving back to the Boarding House.

- Houseparents will ensure that mobile devices are stored safely overnight and during the school day.

- Boarders will have access to their mobile device from 19:30 in the evening. Mobile device access time is structured by year groups in order to reflect the age of the children.

- When a boarder is bringing collected from the Boarding House for the weekend or on an exeat weekend, mobile devices will be returned to the boarder when they are signed out on the register.

- Should a Boarder break any of the House rules in may be that mobile device time is reduced for removed for a limited period.

- The Boarding House mobile or landline are available to Boarders to use should they require.

Pupil Mobile Device Schedule for <u>Day Pupils</u>

- "Mobile Device Parent/Guardian Permission form" **<u>and</u>** "Pupil Mobile Device Contract for Day Pupils" must be signed day pupils are allowed to bring in their mobile device.

- Mobile devices must be handed into the member of staff on duty as soon as day pupils arrive at school before Tutor time.

- Members of the duty team will ensure that mobile devices are stored safely during the school day.

- Mobile devices will be available for collection at the end of the school day. A member of staff on duty will supervise this in the main entrance to Oak House.

- Should a day pupil need to contact home during the school day they should ask at reception if the school landline may be used.

Pupil Mobile Device Schedule for <u>School Trips</u>

- Mobile devices may be used for the travel leg of a school trip, should the journey be deemed long enough to warrant this. This decision will be made by the organiser of trip and arrangements will be made clear to both parents and children in advance of the trip.
- Upon arrival at the destination of the trip mobile devices will be collected by staff and kept in a secure location for the duration of the stay or visit.
- Upon departure mobile devices will be returned to each child for the return journey.

Pupil Mobile Device Contract for <u>Day Pupils</u>

- My name must be on my mobile device and I am responsible for looking after my mobile device when in use.
- I am responsible if my mobile device gets lost or broken.
- I will only give my mobile number to my friends and I will never share other peoples' mobile numbers to anyone.
- I will not take photographs/videos/recordings of any pupil or staff at any time.
- If I need to call home during the school day, I will ask reception to contact my parent/carer.
- I will hand my device to the member of staff on duty each morning when I arrive at school, before Tutor time.
- I will collect my device at the end of the school day from the member of staff on duty from the entrance to Oak (reception).
- The Headmaster or Head of Pastoral may search my device if he/she feels it necessary and I understand that if I use my mobile device to look at anything inappropriate, I will have my device confiscated by a member of staff. My parents will be informed and it will not be returned to me until an investigation is concluded.
- I will not <u>upload</u> any data. School work can be shared on Student Shared.
- I understand that using a device to bully or threaten other pupils is not allowed and that 'ganging-up' on anyone, or cyber bulling is not allowed. I will have my mobile device confiscated if I do this.
- I will inform a staff member if I become aware of another pupil using their mobile device inappropriately.
- I understand that I am no allowed to use my phone during the school day
- I agree to these rules.

Print Pupil Name……

Pupil Signature…… Date……

Appendix 2– Staff and Directors ICT Acceptable Use Policy

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's Online 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 online safety Lead (Mrs Julia Hendrickse)
- 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 pupils 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 pupils 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 Mr David King Headmaster. (See Data protection 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 Online safety Officer, (Mrs Julia Hendrickse), 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 online 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 Online safety Officer. I will not access any material that the Online 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 pupils 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 - Mobile and Smart Technology Policy, including taking and storing images of pupils

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. 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 allegation;
- 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 website, 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. Pupils' 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 alter their privacy settings to block their number.

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 social media 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 staff not to accept friend requests from pupils until they are 18 years of age and have been out of school for three years.

Guidance on Use of Mobile Devices by Pupils (3G, 4G and 5G access): The school recognises that by using devices which have access to 3G, 4G and 5G mobile phone networks, this can result in children having unlimited and unrestricted access to the internet, which could lead to some children, whilst at school or college, sexually harassing their peers via their mobile and smart technology, sharing indecent images: consensually and non-consensually (often via large chat groups), and viewing and sharing pornography and other harmful content. The school takes precautions to ensure that pupils limit access to their personal mobile devices in boarding, and reserves the right to confiscate and monitor personal devices when deemed necessary for safeguarding concerns. Parent's sign a "Mobile Device Parent/Guardian Permission" form to confirm that parental controls are set up on my child's devices with the correct age appropriate content filters.

In the boarding houses, mobile phones are permitted during free time, although their use is prohibited after lights out. 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 sharing nudes/semi-nudes (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 sharing nudes/semi-nudes (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.

Unacceptable Uses: In order to protect one's privacy and respect to others, unless express permission is granted, mobile phones, laptops and mobile devices should not be used to make calls, send messages, use the internet, take photos or use any other application during school lessons, other educational activities such as assemblies, or in the Appleford School Dining Halls.

- radicalise others or breach copyright laws is unacceptable. Cyber bullying will not be tolerated. In some cases, it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given (Please refer to our Anti-bullying Policy);
- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow pupils, staff or visitors to the school;
- Any pupil who uses vulgar, derogatory, or obscene language while using a mobile phone may face disciplinary action;
- Safeguarding, privacy and respect are paramount at Appleford School. To this end, it is prohibited to take a picture of or record a member of staff without their permission. In the event that this happens the pupil will be asked and expected to delete those images and may be requested to turn over the device to the Headmaster and/or the Designated Safeguarding Lead;
- Pupils are reminded that 'sending nudes/semi-nudes' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. Pupils must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. 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.

This may result in disconnection from the school 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.

Additionally, school staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device,staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, Prevent lead or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of a school discipline), and/or
- Report it to the police

Theft or damage: Mobile phones or any mobile devices that are found in the school and whose owner cannot be located should be handed to Reception. The school accepts no responsibility for replacing lost, stolen or damaged devices. The school accepts no responsibility for damage to or loss of mobile phones or mobile devices while travelling to and from school. **It is strongly advised that pupils use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones or other mobile devices. Pupils must keep their password/pin numbers confidential.**

Inappropriate conduct in exams: Under exam regulations, mobile phones are prohibited from all examinations. Pupils MUST give phones to invigilators before entering the exam hall. Any pupil found in possession of a mobile phone during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.

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 website: 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 2021'). 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 parents, volunteers and visitors (including taking and storing images): 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. 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. The exception to this would be at an organised event. 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. *"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 Data Protection Laws. 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 Data Protection."* If they wish to make or take an emergency call they may use the office and the school phone.

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.

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

Online safety FAQs

How will the policy be introduced to Pupils?

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

How will ICT system security be maintained?

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

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

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

How will complaints regarding Internet use be handled?

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

How will parents' support be enlisted?

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

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

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

How is the Safe Use of ICT and the Internet Promoted? 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 Online safety Officer and IT Department;
- Staff and Pupils should ensure that their use of Internet derived materials complies with copyright law;
- Pupils should be taught to be critically aware of the materials they read and show how to validate information before accepting its accuracy;
- Pupils will be taught to acknowledge the source of information used and to respect copyright.

How is Filtering Managed? Having Internet access enables pupils to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. All unsuitable websites will

be filtered and automatically blocked by our security system (Smoothwall) and will not be made accessible to pupils. In addition, pupils' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert our DSL. The IT Department will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of pupils. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at 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 Online safety Officer and ICT Coordinator immediately;
- The school will take every step to ensure that appropriate filtering systems are in place to protect pupils from unsuitable material and the methods used will be reviewed regularly;
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk).

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

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

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

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

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

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

How is Printing Managed?

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

What are the categories of Cyber-Bullying?

Seven categories of cyber-bullying have been identified:

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

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

The following will apply:

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

What are the Pupil Rules?

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

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

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

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

- Between a fifth and a quarter of pupils have been cyber-bullied at least once over the previous few months;
- Phone calls, text messages and email are the most common forms of cyber-bullying;
- There is more cyber-bullying outside school than in;
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone;
- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying;
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying;
- Website and text bullying are equated in impact to other forms of bullying;
- Around a third of those being cyber-bullied tell no one about the bullying.

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

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

How do I stay secure on the Internet?

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

Why is Promoting Safe Use of ICT Important?

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, visitors and parents/carers;
- How we inform parents/carers, visitors and other professional of our procedures;
- What type of mobile phones will be used on educational visits and learning outside the classroom;
- The consequences of any breaches of this policy;
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

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

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

We ensure pupils are safe from terrorist and extremist material when accessing the Internet in school, including by ensuring suitable filtering is in place. The DfE advises that Internet safety will usually be integral to the ICT curriculum and can also be embedded in

PSHEE, for example. Every teacher needs to be aware of the risks posed by online activity of extremist and terrorist groups. For further information, please refer to our *'Preventing Extremism and Radicalisation'* Policy.

Prevent – Top ten FAQs

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

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

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

2. What do we have to do?

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

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

Demonstrate effective leadership: display an awareness and understanding of the risk of radicalisation in your area and institution; communicate and promote the importance of the *Prevent* duty to staff; ensure staff implement the *Prevent* duty effectively.
Train staff: ensure staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism; ensure staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism and are shared by terrorist groups; ensure staff know where and how to refer pupils and young people for further help.
Work in partnership with other agencies: co-operate productively, in particular, with local *Prevent* co-ordinators, the Police and local authorities, and existing multi-agency forums, for example Community Safety Partnerships; ensure that safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Children's 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
Laptop Computer Device Contract
Parent/Guardian Permission

I have read and understand the mobile devices acceptable use policy about appropriate use of laptop devices at Appleford School and I understand that this form will be kept on file at the school and that the details may be used (and shared with a third party, if necessary) to identify a laptop computer should the need arise (e.g. if lost, or if the laptop is being used inappropriately).

I give my child permission to carry a laptop computer device to school and understand that my child will be responsible for ensuring that the laptop computer device is used appropriately and correctly while under the school's supervision, as outlined in this document.

I understand that the school will not accept any responsibility for loss, damage or theft of a laptop computer device.

I understand that my child will not be allowed a laptop computer device in school unless this form has been completed in full, signed and returned.

Computer Contract
All pupils

Name of Parent/carer: (Please print)	
Name of pupil: (Please print)	

Mobile device details:

Make and model number ……

Size ……

Colour/description of laptop ……

I confirm that parental controls are set up on my child's devices with the correct age appropriate content filters.

Android link: Family Link from Google - Family Safety & Parental Control Tools (families.google)

Apple link: Share with your family – Apple Support (UK)

For Boarding pupils
Tick here if you wish your child to have access to his/her laptop in boarding time. ☐

Parent name: ……

Parent Signature: ……

Date: ……

Pupil Mobile Laptop / Tablet Contract for Pupils

- My name must be on my laptop computer device and I am responsible for looking after my laptop computer device when in use.
- I am responsible if my laptop computer gets lost or broken.
- When using my laptop computer in school, I will only access lesson content and use the laptop for the intent of supporting my learning.
- I will hand my laptop computer into the Admin office over the lunch break, and return to collect it before the afternoon lessons begin.
- I will not take photographs/videos/recordings of any pupil or staff at any time.
- I will never use my laptop computer device in the dorms or toilets.
- I will have my device collected before bedtime and kept overnight by the Houseparents. The Houseparents also have the right to decide when and where any devices can be used.
- The Headmaster or Head of Boarding may search my laptop computer if he/she feels it necessary and I understand that if I use my laptop computer to look at anything inappropriate, I will have my laptop confiscated by a member of staff. My parents will be informed and it will not be returned to me until an investigation is concluded.
- I will not upload any data. School work can be shared on Student Shared.
- I understand that using a laptop computer to bully or threaten other pupils is not allowed and that 'ganging-up' on anyone, or cyber bulling is not allowed. I will have my laptop computer device confiscated if I do this.
- I will inform a staff member if I become aware of another pupil using their laptop computer inappropriately.
- I agree to these rules.

Print Pupil Name……

Pupil Signature…… Date……

Appendix 6

WhatsApp Agreement
Parent/Guardian Permission
(for overseas boarders)

While WhatsApp as an application is given an official '13+' rating by the NSPCC, it is understood that many children under 13 use the app to contact friends and family. When in the boarding environment, this application is not to be used by any child under the age of 13, as per the recommendations of the NSPCC.

As a free and popularly used application amongst adults around the world, it is natural that this is the application of choice for children from overseas for them to keep in contact with friends and family abroad, and therefore special permission has been granted to allow this child to use WhatsApp in boarding time.

However, in signing this agreement, they agree to adhere to a usage policy as defined below:

- I will only contact friends (out of school) and family members on WhatsApp.
- I will not use WhatsApp to contact any school or boarding friends in boarding time, understanding that they are not allowed to access the app for anything other than family contact.
- I will not accept group requests or chat requests from numbers I have not got saved in my phone.
- I will share any worrying messages with a parent or member of the boarding team immediately.

Name of Parent/carer: (Please print)	
Name of pupil: (Please print)	
Date:	

Any breeches of this usage policy will result in the loss of this privilege.

Pupil signature:…….