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.

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

Signed: Policy Agreed: January 2025

Date Published: J a n u a r y 2025 Next Review: September 2025

Dr Peter Gardner (Proprietor) **Mr David King (Headteacher)**

This policy will be reviewed no later than September 2025, or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.

Page Contents

1. Monitoring and Review;
2. Introduction, Roles and Responsibilities;
3. Designated Safeguarding Lead; Staff; Parents; Pupils; Staff/Volunteers Use of IT Systems;
4. Teaching and Learning, Teaching about Online Safety; Educating Staff;
5. Educating Parents, Protecting Personal Data;
6. Assessing Risks; Mobile Electronic Device; Cyber-Bullying;
8. Online Sexual Harassment; ICT-Base Sexual Abuse (Inc Sexting);
9. Chat Room Grooming and Offline Abuse; Social Media; Use of Email;
10. Taking and Storing Images of Pupils; Remote Learning;
11. Related Documents; Legislation and Guidance;

Introduction: The primary purpose of this Policy is to safeguard pupils and staff at the 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 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 & 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 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 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 Operation Management Team (OMT and the 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 and
- 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 SMT. 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 (and 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 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;
- 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 the school'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, and ensuring that pupils follow the school's terms on **acceptable use agreement**
- Working with the DSL and/or **prevent lead** to ensure that any online safety incidents are logged 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.
- 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

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.

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.

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.

Pupils Use of IT Systems: All pupils must agree to the IT Acceptable Use Policy before accessing the school systems. Pupils at Appleford 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. The 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)

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. The 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 will also be provided with a copy of the Pupil IT Acceptance Policy, and parents will be asked to sign it, as well as pupils aged eight and older. 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: 2023) and uses these as a base for keeping the school and its community safe from cyber-crime**.**

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.

The 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: We have 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. The 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;

- The 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";
- The 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 the leadership team 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: 2024) 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 technology and techniques designed to prevent them is crucial. A plethora of reliable educational resources exist 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 Centre

Mobile and Smart Technology (Phones, Laptops, iPads and Tablets): 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. The School is not responsible for any devices lost by pupils. (See Safeguarding Children-Child Protection policy).

Cyber-Bullying: 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.

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.

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
- The 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): Appleford 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 on taking and storing of photos. 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 the 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 the 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, Appleford 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;
- 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 2024) 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: 2024) (including Broadband, Cyber-Security and data protection procedures)
- Filtering and monitoring standards for schools and colleges (DfE: 2024)
- Cyber security standards for schools and colleges (DfE: 2024)
- Promoting and supporting mental health and wellbeing in schools and colleges (September 2022)
- 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