



Policy No. 1.6

APPLEFORD SCHOOL ONLINE SAFETY POLICY

This policy, which applies to all staff, volunteers, contractors and visitors working with pupils in education or the boarding provision publicly available on the school website, on the staff share 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. This policy reflects current legislation, the new recording/parent notification duties and emerging DfE/Ofsted/ISI expectations for residential special schools

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.

This policy applies in:

- classrooms and learning spaces;
- residential accommodation and during the boarding routines;
- on-site and off-site activities, including trips, transport and work experience.

The school is committed to:

- promoting positive relationships, de-escalation and non-restrictive approaches as the norm;
- minimising, and where possible eliminating, the use of restraint and other restrictive interventions;
- ensuring any use of force is lawful, necessary, proportionate, in the child's best interests and a last resort.

Monitoring and Review: The text of this policy is necessary and proportionate to meet the needs of Appleford School, supporting those who work with our pupils, making clearer the responsibilities of school staff, volunteers, proprietor and the Advisory Board. This policy is designed to support the Appleford School staff who work with our pupils who have special educational needs and disabilities (SEND) making clear the responsibilities of school staff, and the proprietor. These arrangements are subject to continuous monitoring, refinement, and audit by Dr Peter Gardner (Proprietor and Managing Director), and Mr David King (Headmaster and Non-Executive Director).

The Proprietor and Headmaster are committed to regularly reviewing and updating our policies to ensure they remain relevant and effective in supporting our school's mission and values, inclusive of its implementation and the efficiency with which the related duties have been implemented. Any amendments, where appropriate, will be made in consultation with staff, the Proprietor, and/or the wider school community to reflect our ongoing commitment to excellence in education. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements, and it will be made available to them in writing or electronically

Policy Updated and Agreed: September 2026

Date Published: September 2026

Next Review: September 2027

Signed

Dr Peter Gardner
Proprietor and Managing Director

Mr James Lanagan
Headmaster

Separate Support Documents integral to the Online Safety policy:

- 1, Mobile Devices inclusive of Bring Your Own Device (BYOD);
- 2, Cyber Security Policy;
- 3, Photography and Images Policy;
- 4. Social Media Policy;
- 5. Safe Use of Artificial Intelligence Policy (AI)

Statement of intent: Appleford believes that it is important to establish a safe, secure and stable environment to enable pupils to grow, develop and learn. The school takes a proactive approach to anticipating, managing and minimising potential triggers of distressed behaviour that may cause harm. The aim of this policy is to ensure that mobile devices inclusive of BYOD are used in a correct and safe manner, which is in accordance with the relevant legislation and national guidance.

Where this policy refers to “must”, it reflects legal duties or statutory guidance; “should” reflects best practice. Appleford understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff. The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal framework: Legal and regulatory framework: This policy is informed by, and should be read alongside, all relevant legislation and statutory guidance including, but not limited to, the following:

- Keeping children safe in education 2026 (DfE September 2026) <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2> Teaching Online Safety in Schools (DfE January 2023) <https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools>
- Preventing and Tackling bullying (DfE July 2017) <https://www.gov.uk/government/publications/preventing-and-tackling-bullying>
- Cyber Bullying: advice for Headmasters and school staff (DfE July 2017) <https://www.gov.uk/government/publications/preventing-and-tackling-bullying>
- Searching, screening and confiscation at school (DfE July 2022) <https://www.gov.uk/government/publications/searching-screening-and-confiscation#full-publication-update-history>
- The Prevent duty: safeguarding learners vulnerable to radicalisation (DfE September 2023) <https://www.gov.uk/government/publications/the-prevent-duty-safeguarding-learners-vulnerable-to-radicalisation>
- Data Protection Act 2018 (HM Gov June 2018) <https://www.legislation.gov.uk/ukpga/2018/12/contents>
- The UK General Data Protection Regulation (UK GDPR) (HM Govt: currently in force) <https://www.legislation.gov.uk/eur/2016/679/contents>
- Voyeurism (Offences) Act 2019 (HM Gov April 2019) <https://www.legislation.gov.uk/ukpga/2019>
- Online Safety Act 2023 (HM Gov October 2023) <https://www.legislation.gov.uk/ukpga/2023/50/2026-04-29>
- Filtering and monitoring standards for schools and colleges (DfE March 2022) <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>

- Harmful online challenges and online hoaxes (DfE February 2021) <https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes>
- Generative artificial intelligence in education (DfE August 2025) <https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education>
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UK Gov March 2024) <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>

It also reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting

This policy operates in conjunction with the following school policies

- | | |
|---|--|
| • Child protection and safeguarding policy | • Cyber Response and Recovery Plan |
| • Positive Behaviour Management policy | • Child Protection and Safeguarding Policy |
| • Staff Behaviour Policy (Code of Conduct) inclusive of the Staff disciplinary procedures | • Child-on-child Abuse Policy |
| • Data protection policy and privacy notices | • Anti-Bullying Policy |
| • Complaints procedure | • Data Protection Policy |
| • ICT and internet acceptable use policy | • Confidentiality Policy |
| • Social Media Policy | • Photography and Images Policy |
| • Allegations of Abuse Against Staff Policy | • Device User Agreement |
| • Technology Acceptable Use Agreement | • Staff ICT and Electronic Devices Policy |
| • Cyber-security Policy | • Prevent Duty Policy |
| • Restrictive Physical Interventions | • Remote Education Policy |
| • Mobile Phone inclusive of Bring Your Own Device (BYOD); | |
| • Medical Conditions and Allergies | |
| • Low Level Concerns. | |
| • Special Educational Needs and Disabilities (SEND) | |
| • Photography and Images Policy | |
| • Social Media Policy | |
| • Safe Use of Artificial Intelligence Policy (AI) | |
| • Searching, Screening and confiscation Policy | |

Roles and responsibilities

The proprietor will be responsible for:

- ensuring that this policy is effective and complies with relevant laws and statutory guidance;
- ensuring the Designated Safeguarding Lead's (DSL) remit covers online safety;
- reviewing this policy annually;
- ensuring their own knowledge of online safety issues is up to date;
- ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular interval;
- ensuring that there are appropriate filtering and monitoring systems in place;
- ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers;
- ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified;
- ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them and
- ensuring compliance with the DfE's 'meeting digital and technology standards in schools and colleges', regarding the filtering and monitoring standards in relation to safeguarding.

The headmaster will be responsible for:

Appleford School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all children fulfil their potential

- ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding;
- supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety;
- ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training;
- ensuring online safety practices are audited and evaluated;
- organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe;
- working with the DSL and ICT technicians to conduct a half-termly review of this policy;
- working with the DSL and proprietor to update this policy on an annually;
- identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems and
- appointing a SLT digital lead in line with the cyber-security policy.

The DSL will be responsible for:

- taking the lead responsibility for online safety in the school;
- undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with send face online;
- liaising with relevant members of staff on online safety matters, e.g. the SENCo and ICT technicians;
- ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented;
- ensuring safeguarding is considered in the school's approach to remote learning;
- establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure;
- understanding the filtering and monitoring processes in place at the school.
- ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school;
- maintaining records of reported online safety concerns as well as the actions taken in response to concern;
- monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures;
- reporting to the proprietor about online safety on a termly basis;
- working with the headmaster and ICT technicians to conduct half-termly light-touch reviews of this policy and
- working with the headmaster and governing board to update this policy annually.

ICT technicians will be responsible for:

- providing technical support in the development and implementation of the school's online safety policies and procedures.
- implementing appropriate security measures as directed by the headmaster;
- ensuring that the school's filtering and monitoring systems are updated as appropriate and
- working with the DSL and headmaster to conduct half-termly light-touch reviews of this policy.

All staff members will be responsible for:

- taking responsibility for the security of ICT systems and electronic data to which they have access;
- modelling good online behaviours;
- maintaining a professional level of conduct in their personal use of technology;
- having an awareness of online safety issues;
- ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online;
- reporting concerns in line with the school's reporting procedure and
- where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- adhering to the acceptable use agreement and other relevant policies;
- seeking help from school staff if they are concerned about something they or other pupils have experienced online and
- reporting online safety incidents and concerns in line with the procedures within this policy.

Appleford School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all children fulfil their potential

Managing online safety: All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet. The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the **headmaster** where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff, proprietor and Advisory board receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are regularly conducted on the topic of remaining safe online

Handling online safety concerns: Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy. Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully. The reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered. Concerns regarding a staff member's online behaviour are reported to the headmaster, who decides on the best course of action in line with the relevant policies. If the concern is about the headmaster, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headmaster and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headmaster contacts the police. The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and because of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy. All online safety incidents and the school's response are recorded by the DSL.

Cyberbullying: Cyberbullying can include, but is not limited to, the following:

- threatening, intimidating or upsetting text messages;
- threatening or embarrassing pictures and video clips sent via mobile phone cameras;
- silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;
- threatening or bullying emails, possibly sent using a pseudonym or someone else's name;
- unpleasant messages sent via instant messaging;
- unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. facebook;
- abuse between young people in intimate relationships online i.e. teenage relationship abuse and
- discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as lesbian, gay, bisexual, or gender questioning pupils and pupils with SEND. Cyberbullying against pupils or staff is not tolerated under any circumstances.

Appleford School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all children fulfil their potential

Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying: To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. Please see our Anti-bullying Policy for more detail. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teacher and mentors will discuss cyber-bullying with their mentor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic education (PSHEE), and other subjects where appropriate. All staff, appropriate Directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy and Anti-

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices: The Headmaster, and any member of staff authorised to do so by the headmaster, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting that it: poses a risk to staff or pupils, and/or;

- is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL;
- explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it and
- seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- cause harm, and/or undermine the safe environment of the school or disrupt teaching, and/or commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- not view the image;

- confiscate the device and report the incident to the DSL immediately, who will decide what to do next. the DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK council for internet safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- the DfE's latest guidance on searching, screening and confiscation;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- our behaviour policy and
- confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Child-on-child sexual abuse and harassment: Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware of:

- threatening, facilitating or encouraging sexual violence;
- upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks;
- sexualised online bullying, e.g. sexual jokes or taunts;
- unwanted and unsolicited sexual comments and messages;
- consensual or non-consensual sharing of sexualised imagery and
- abuse between young people in intimate relationships online, i.e. teenage relationship abuse.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct. Creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

Appleford is aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy, Child Protection and Safeguarding Policy, and the social media Policy. We respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

Grooming and exploitation: Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion. Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- being secretive about how they are spending their time online;
- having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met and having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Appleford School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all children fulfil their potential

Child sexual exploitation (CSE) and child criminal exploitation (CCE): Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking. CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence.

While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet. Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation: Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised. Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

Mental health: Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Online hoaxes and harmful online challenges: For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms. For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same.

Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly because of partaking in the challenge itself or indirectly because of the distribution of the video online. The latter will usually depend on the age of the pupil and the way in which they are depicted in the video. Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely. Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headmaster will decide whether each proposed response is:

- in line with any advice received from a known, reliable source, e.g. the UK safer internet centre, when fact-checking the risk of online challenges or hoaxes;
- careful to avoid needlessly scaring or distressing pupils;
- not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils;
- proportional to the actual or perceived risk;
- helpful to the pupils who are, or are perceived to be, at risk;
- appropriate for the relevant pupils' age and developmental stage;
- supportive and
- in line with the child protection and safeguarding policy.

If the DSL's assessment finds an 'online challenge' to be putting pupils at risk of harm, then the DSL will ensure that the 'online challenge' is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected, or individual pupils at risk where appropriate. The DSL and headmaster will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime: Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests. The DSL and headmaster will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety training for staff: All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. Additionally, the DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils. Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours. Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, online training courses and staff meetings).

By way of this training, all staff will be made aware that:

- technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse;
- children can abuse other children online through:
 - abusive, harassing, and misogynistic messages,
 - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups,
 - sharing of abusive images and pornography, to those who don't want to receive such content,
- physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse;
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up;
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term;

The DSL and DDSs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually. The proprietor and the proprietors nominated person for safeguarding, will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

Online safety and the curriculum: Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Personal Social Health and Economic (PSHE) education
- Relationships Sex and health education (RSHE)
- Citizenship
- Information Communication Technology (ICT) – Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks: Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks: The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks: Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks: The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity. The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for looked after children (LAC), will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need. The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils. Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headmaster and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Appleford School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all children fulfil their potential

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy. If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom: A wide range of technology will be used during lessons, including the following:

- computers
- laptops
- tablets
- intranet
- email
- cameras
- physical coding devices (e.g. Microbits)

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law. Pupils will be supervised when using online materials during lesson time. This supervision is suitable to their age and ability.

Use of smart technology: While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages. Appleford School is a mobile phone-free environment. In line with DfE guidance 'Mobile Phones in Schools' (January 2026), the school prohibits the use of mobile phones and other smart technology with similar functionality throughout the school day, including during lessons, the time between lessons, breaktimes, and lunchtime. This applies to all devices capable of sending or receiving notifications or messages via mobile phone networks or recording audio and/or video.

Mobile phones are permitted in boarding houses only. Personal devices will not be used at any point during the school day, including during break and lunch times, unless an agreed exception applies. Where an agreed exception is in place, use of a personal device will be limited strictly to the specific purpose outlined within that exception and will be subject to any conditions set by the school. Exceptions are expected to be rare and will be tied to welfare and/or clearly defined operational needs. Authorised exceptions must not distract or disrupt lessons, private study, movement between lessons, or supervision routines.

All other pupils must deposit their mobile phone with their houseparent, or at school reception on arrival in the morning. They are then stored in a secure cabinet in a staff only room. The mobile phones can be collected upon departure at the end of their school day.

Ownership and responsibility: Pupils are responsible for adhering to the provisions outlined in this policy. Pupils are responsible for their own belongings. The school accepts no responsibility for replacing property that is lost, stolen or damaged either on school premises or travelling to and from school, and at school events. Staff will be protected against liability in any proceedings brought against them for any loss or damage to personal devices that have been confiscated as an appropriate sanction, if they have acted lawfully.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils. Staff will use all smart technology and personal technology in line with the school's Staff ICT and Electronic Devices Policy. The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- using mobile and smart technology to sexually harass, bully, troll or intimidate other pupils
- sharing indecent images, both consensually and non-consensually and

Appleford School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all children fulfil their potential

- viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom. Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site. Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy. The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats. The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Staff using work devices outside school: All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- making sure the device locks if left inactive for a period of time;
- not sharing the device among family or friends;
- installing anti-virus and anti-spyware software;
- keeping operating systems up to date – always install the latest updates.

School devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the schools IT technician

Educating parents: The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- child sexual abuse, including grooming;
 - exposure to radicalising content;
 - sharing of indecent imagery of pupils, e.g. sexting;
 - cyberbullying;
 - exposure to age-inappropriate content, e.g. pornography and
 - exposure to harmful content, e.g. content that encourages self-destructive behaviour.
-
- Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content. This awareness regarding how they can support their children to be safe online will be raised in the following ways: Parents' evenings including teams for parents who cannot travel to school
 - Twilight training sessions
 - Newsletters
 - Online resources
 - Parent Portal
 - Online Safety Hub
 - Smoothwalls Qustodio

Internet access: Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office. All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity: The Headmaster, proprietor and DSL will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. Appleford uses Smoothwall as part of its filtering protection.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs. The headmaster, DSL and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headmaster. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police. The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Teaching staff are encouraged to use AB tutor in their classroom

Network security: Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT technicians. All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in class, year or key stage and above will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum of 16 characters and a maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headmaster will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use. The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL. Full details of the school's network security measures can be found in the Cyber-security Policy.

Emails: Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff and Volunteer Confidentiality Policy. Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT technicians will run an annual phishing campaign where they explain what a phishing email and other malicious emails might look like – they will also include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

Generative artificial intelligence (AI): Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Appleford school recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The school will treat any use of AI to bully pupils very seriously, in line with our anti-bullying & behaviour policy. Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff. The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school recognises the educational potential of generative AI tools while being mindful of safety considerations. The school follows the DfE's "Generative AI: product safety expectations" guidance and ensures that:

- Filtering and monitoring requirements apply to the use of generative AI tools in education
- Staff assess age-appropriateness before introducing AI tools to pupils
- Pupils are taught critical thinking skills to evaluate AI-generated content
- Privacy implications are considered when using AI tools that may process personal data
- Staff understand that AI tools should supplement, not replace, teacher expertise and judgment

Any use of generative AI tools will be in accordance with the school's AI Usage Policy and data protection requirements. Staff should be aware that AI-generated content may contain inaccuracies, biases, or inappropriate material, and should review AI outputs before sharing with pupils.

Staff are only permitted to use Copilot and Chalkie on school IT systems. Pupils do not have access to Generative AI tools on school IT equipment.

Social networking: The use of social media by staff and pupils will be managed in line with the school's social media policy.

Reasonable adjustments and individual circumstances: The school recognises its duties under the Equality Act 2010 and the Children and Families Act 2014. Where a pupil has a disability or medical condition that requires the use of a mobile phone during the school day (for example, continuous glucose monitoring linked to a smartphone for pupils with diabetes), this will be agreed with parents, documented, and managed through the pupil's individual healthcare plan or SEND provision. Where a pupil's individual circumstances require access to a mobile phone during the school day (for example, a young carer), the school will agree specific arrangements for the pupil to use their phone at designated times and in the pastoral care office.

The school website: The Headmaster will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. The website will be managed in line with the School Website Policy.

Use of devices: Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement. The use of personal devices on the school premises and for the purposes of schoolwork (curriculum and associated activities) will be managed in line with the Staff ICT and Electronic Devices Policy and Pupils' Personal Electronic Devices Policy.

School trips and activities Learning Outside the Classroom (LOtC): The school will determine the appropriate arrangements for pupil phone use on residential trips, day trips, and activities outside the normal school day. The default position is that the school's phone-free approach applies unless the trip leader, in agreement with SLT, determines that specific arrangements are necessary. Details will be communicated to parents and pupils in advance of the trip.

Remote learning: All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education. Pupils are entitled to remote learning when the school is closed to pupils during term time and if a pupil is unable to attend school due to other extenuating circumstances (this arrangement is agreed on a case-by-case basis between the parents/guardians and the headmaster). In these circumstances, the school recognises its responsibility to keep pupils safe online and follow the advice pages hyperlinked in:

- Keeping Children Safe in Education in our guidance for staff, which they are issued as a remote learning agreement:
- Safeguarding and remote education - GOV.UK (www.gov.uk)
- Undertaking remote teaching safely | NSPCC Learning

Pupils are also provided with a remote learning agreement which they are asked to read before commencing remote learning for any period of time. This agreement primarily focuses on acceptable behaviours whilst working remotely and staying safe online. The remote learning agreements for staff and pupils are available on request. At Appleford, we recognise that during periods of remote learning it is our responsibility to stay in regular contact with parents and carers, to reinforce the importance of ensuring that their child is staying safe online and what their child is being asked to do.