LEASOWES EXTRA
Online Safety Policy

Date approved: March 2026	**Written by: J.Caven** **Business Manager**
Date to be Reviewed: March 2027	**Approved by: G.Bettany** **Chair of Trustees**

Contents

Statement of Intent

Leasowes Extra understands that using online services is an important aspect of raising educational standards, promoting child achievement, and enhancing teaching and learning. The use of online services is embedded throughout the setting; therefore, there are a number of controls in place to ensure the safety of children 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, fake news, 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.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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

1. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2025) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE 'Keeping children safe in education' (2025)
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'
- UK Council for Internet Safety (UKCIS): 'Education for a Connected World – 2020 edition'

This policy should be read in conjunction with these other setting policies:

- Allegations of Abuse Against Staff Policy
- Low-level Safeguarding Concerns (Staff)
- Safeguarding and Child Protection Policy (including Prevent)
- Anti-Bullying Policy
- Staff Code of Conduct
- Behavioural & Discipline Policy
- Disciplinary Policy
- Data protection Policy
- Technology Acceptable Use Agreement - for Parents and Children
- Technology Acceptable Use Agreement – Staff
- Photograph and Video Consent Policy

2. Roles and Responsibilities

The Trustees are responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance
- Ensuring the DSL's remit covers online safety
- Reviewing this policy on an annual basis
- 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
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that all relevant setting policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Business Manager is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the setting's policies and procedures, including in those related to safeguarding.
- Supporting the any deputy DSL's 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
- Supporting staff to ensure that online safety is embedded throughout the EYFS curriculum so that all children can develop an appropriate understanding of online safety
- Engagement with parents to keep them up-to-date with current online safety issues and how the setting is keeping children safe
- Working with the Trustees to update this policy on an annual basis

The DSL is responsible for:

- Taking the lead responsibility for online safety in the setting
- Acting as the named point of contact within the setting on all online safeguarding issues
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that children 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 setting's safeguarding responsibilities and that a coordinated approach is implemented
- Ensuring safeguarding is considered in the setting's approach to remote learning
- Ensuring appropriate referrals are made to external agencies, as required
- Working closely with the police during police investigations
- Keeping up-to-date with current research, legislation and online trends
- Encouraging participation in local and national online safety events, e.g. Safer Internet Day
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by children and staff
- Ensuring all members of the setting understand the reporting procedure
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns
- Monitoring online safety incidents to identify trends and any gaps in the setting's provision, and using this data to update the setting's procedures
- Reporting to the Trustees about online safety
- Working with the Trustees to update this policy on an annual basis

The Technical Staff & Co-ordinator for Computing in the school are responsible for ensuring:

- That the setting's technical infrastructure is secure and is not open to misuse or malicious attack
- That the setting meets required online safety technical requirements and any guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection procedure
- The filtering procedure is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Business Manager/Online Safety Coordinator in school for investigation, action and sanction
- That monitoring software systems are implemented and updated as agreed in the setting/school policies

All staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current setting Online Safety Policy and practices
- They have read, understood and signed the Staff & Volunteer Technology Acceptable Use Agreement
- They report any suspected misuse or problem to the Business Manager/Online Safety Coordinator in school for investigation, action and sanction
- Reporting incidents quickly and efficiently
- All digital communications with children, parents/carers should be on a professional level and only carried out using official setting systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Children understand and follow the Online Safety Policy and acceptable use agreements
- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in all setting activities and implement current policies with regard to these devices
- During learning and recreation where internet use is planned, children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Modelling good online behaviours

Children are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from setting staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy

3. Parents / Carers

The setting works in partnership with parents to ensure children stay safe online whilst in the setting and at home. Parents are provided with information about the setting's approach to online safety and their role in protecting their children. The Acceptable Use Agreement is shared with all parents, who 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 children, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- 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.
Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Website
- Newsletters
- Online resources
- Literature

Parents and carers will be encouraged to support the setting in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at setting events
- Access to parents' sections of the website and on-line child records
- Any remote learning

4. 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 setting's approach to online safety, with support from deputies and the Trustees where appropriate, and will ensure that there are strong processes in place to handle any concerns about children' 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 setting operations in the following ways:

- Staff and Trustees 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
- In school, assemblies are conducted on the topic of remaining safe online and 'drip fed' throughout other assemblies

Handling online safety concerns
Any disclosures made by children 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 Safeguarding and Child Protection Policy.
Staff will be aware that children may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.
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 children 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 in order 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 and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the Business Manager, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Business Manager, it is reported to the Chair of the Trustees.

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

Where there is a concern that illegal activity has taken place, the DSL contacts the police.

The setting avoids unnecessarily criminalising children, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a child 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 Safeguarding and Child Protection Policy.

All online safety incidents and the setting's response are recorded by the staff/DSL on my concern.

5. 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
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The setting will be aware that certain children can be more at risk of abuse and/or bullying online, such as LGBTQ+ children and children with SEND.

Cyberbullying against children or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

6. Child-on-child sexual abuse and harassment

Children 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 setting, off and online, and will remain aware that children 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:

- 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
- 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 setting culture that normalises abuse and leads to children becoming less likely to report such conduct.

Staff will be aware that 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.

The setting will be 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 children taking "sides", often leading to repeat harassment. The setting will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The setting responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the setting premises or using setting-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the settings Safeguarding and Child Protection Policy.

7. 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 children who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The child believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The child does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The child may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the child feel 'special', particularly if the person they are talking to is older.
- The child 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 children 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.
- Having an older boyfriend or girlfriend, usually one that does not attend the setting and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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 child 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 children 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 Safeguarding and Child Protection 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 children at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any children displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a child relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty and Radicalisation information contained within the Safeguarding and Child Protection Policy. All teaching staff complete regular Prevent training.

8. Mental Health

The internet, particularly social media, can be the root cause of a number of mental health issues in children, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of setting can have a substantial impact on a child'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 child is suffering from challenges in their mental health. Concerns about the mental health of a child will be dealt with by the DSL.

9. 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 as a result of partaking in the challenge

itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the child 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 children in the setting, 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 children, and whether the risk is one that is localised to the setting 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 Trustees 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 children.
- Not inadvertently encouraging children to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger children but is almost exclusively being shared amongst older children.
- Proportional to the actual or perceived risk.
- Helpful to the children who are, or are perceived to be, at risk.
- Appropriate for the relevant children's age and developmental stage.
- Supportive.
- In line with the Safeguarding and Child Protection Policy.

Where the DSL's assessment finds an online challenge to be putting children at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant children, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.
The DSL and Trustees will only implement a setting-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing children's exposure to the risk is considered and mitigated as far as possible.

10. 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 setting will factor into its approach to online safety the risk that children with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a child's use of technology and their intentions with regard to using their skill and affinity towards it, 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 Trustees will ensure that children are taught how to use technology safely, responsibly and lawfully.

11. Online Training for Staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that children 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.

Information about the setting's full responses to online safeguarding incidents can be found in the Safeguarding and Child Protection Policy.

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 children.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support children in developing critical thinking skills and safe online behaviours.

12. Online Safety and Learning

Online safety is always appropriate to the children' ages and developmental stages.

Children 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 children learn include eight strands of our online lives from early years.

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

The setting recognises that, while any child can be vulnerable online, there are some children who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. children with SEND and/or LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, works to ensure learning is tailored so these children receive the information and support they need.

The setting 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 children.

Practitioners review external resources prior to using them to ensure they are appropriate for the cohort of children. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for children?
- Are they appropriate for the children's developmental stage?

Before conducting any learning on online safety, practitioners, and wherever necessary the DSL, consider the topic that is being covered and the potential that any children have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any child who may be especially impacted by an activity. Lessons and activities are

planned carefully so they do not draw attention to a child who is being or has been abused or harmed online, to avoid publicising the abuse.
If a staff member is concerned about anything children raise with regard to online safety during their time in the setting, they will make a report in line with the Safeguarding and Child Protection Policy.
If a child makes a disclosure to a member of staff regarding online abuse, the staff member will follow the reporting procedure outlined in the Safeguarding and Child Protection Policy.
Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in online safety is therefore an essential part of the setting's online safety provision. Children and young people need the help and support of the setting to recognise and avoid online safety risks and build their digital resilience.
Online safety should be broad, relevant and provide progression and will be provided in the following ways:

- Key online safety messages should be reinforced
- Children should be taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Children should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside setting
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- Children should be taught about the safe and appropriate use of mobile devices
- Children should be guided to sites checked as suitable for their use and processes should be in place for dealing with any unsuitable material that is found in internet searches
- Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

13. Use of Technology in the Setting

A wide range of technology is used in the setting, including the following:

- Computers
- Laptops
- Tablets/iPads
- Internet
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the setting, or recommending that children use these platforms at home, staff always review and evaluate the resource. Practitioners ensure that any internet-derived materials are used in line with copyright law.
Children are supervised when using online materials during activities – this supervision is suitable to their age and ability.

14. Use of Smart Technology

While the setting recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the setting will ensure it manages.

Children will be educated on the acceptable and appropriate use of all devices and will use technology in line with the setting's Technology Acceptable Use Agreement.
Staff will use all smart technology and personal technology in line with the setting's Acceptable Use Agreement – staff.
The setting recognises that children's unlimited and unrestricted access to the internet via mobile phone networks means that some children may use the internet in a way which breaches the setting's acceptable use of ICT agreement for parents and children.
Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Children will not be permitted to use smart devices or any other personal technology whilst at the setting and children who have permission to have a mobile phone will need to hand them in.
Where it is deemed necessary, the setting will ban children's use of personal technology whilst on site.
Where there is a significant problem with the misuse of smart technology among children, the setting will discipline those involved in line with the setting's Behaviour Policy.
The setting will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.
The setting will consider the 4C's (content, contact, conduct and commerce) when educating children about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

15. Filtering and Monitoring Online Activity

The school ensures that the setting'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'. They ensure 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online learning and safeguarding.
The school's ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems they implement are appropriate to children's ages, the number of children using the network, how often children access the network, and the proportionality of costs compared to the risks. ICT technicians undertake **monthly** checks on the filtering and monitoring systems to ensure they are effective and appropriate.
Requests regarding making changes to the filtering system are directed to the Business Manager. Prior to making any changes to the filtering system, ICT technicians and the school DSL conduct a risk assessment. Any changes made to the system are recorded by ICT technicians. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.
Deliberate breaches of the filtering system are reported to the school's DSL and ICT technicians, who will escalate the matter appropriately. If a child has deliberately breached the filtering system, they will be disciplined in line with the setting 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 network and devices are appropriately monitored. All users of this network and these devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Safeguarding and Child Protection Policy.

Our current filtering system is Netsweeper.
Our current monitoring system which is fully managed is Securus.

16. Network Security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the school's ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls on a **weekly** basis to ensure they are running correctly, and to carry out any required updates.
Staff and children are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the ICT technicians.
All members of staff have their own unique usernames and private passwords to access the setting's systems. Children in KS2 will be provided with a username and generate their own secure password. An up-to-date record of users and their usernames will be kept securely. Users are responsible for the security of their username and password and will be required to change their password every academic year or more frequent if there is a password breach. Class logons and passwords will be used for KS1 and EY.
Staff members and children are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords are changed regularly.
Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not 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 Business Manager is informed and decides the necessary action to take.
Users are required to lock access to devices and systems when they are not in use.
Full details of the school's network security measures can be found in their Data and Cyber-security Breach Prevention and Management Plan.

17. Emails

Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable Use Agreement. Staff and children are given approved email accounts and are only able to use these accounts either in school or when completing school/work related tasks outside of normal school hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Any email that contains sensitive or personal information is only sent using secure and encrypted email.
Staff members and children are 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 children are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened. Online safety lessons in school for children with access to emails explain what a phishing email and other malicious emails might look like – this includes 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 are managed in line with the school's Risk Protection Arrangement Cyber Response Plan.

18. Generative Artificial Intelligence

The setting will take steps to prepare children for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to children's age.

The schoool will ensure its IT system includes appropriate filtering and monitoring systems to limit children's ability to access or create harmful or inappropriate content through generative AI.
The setting will ensure that children are not accessing or creating harmful or inappropriate content, including through generative AI.
The setting will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.
The setting will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

19. The School/Setting Website

The Business Manager will be responsible for the overall content of the settings pages on the school's website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

20. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The setting will inform and educate users about these risks to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of children are published on the setting/school website, social media or local press (this is covered by the setting's photographic consent form)
- In accordance with guidance from the Information Commissioner's Office, parents /carers are welcome to take videos and digital images of their children at setting events for their own personal use (as such use is not covered by the Data Protection Act) if the setting gives permission to do so. To respect everyone's privacy and in some cases protection, these images should not be on social networking sites, nor should parents /carers comment on any activities involving other children in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support learning and childcare aims, but must follow setting policies concerning the sharing, distribution and publication of those images. Those images should only be taken on setting equipment and deleted from equipment immediately after use. The personal equipment of staff should never be used for this purpose.
- Care should be taken when taking digital /video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the setting into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.

- Children's full names will not be used anywhere on a website, particularly in association with photographs.
- Children's work can only be published with the permission of the child and parents or carers.

21. Communications

Communication Technologies	Staff & other adults				Children			
	Allowed	Allowed at certain times in designated areas	Allowed for selected staff	Not Allowed	Allowed	Allowed at certain times	Allowed with Permission & handed in	Not allowed
Mobile phones may be brought into the setting	✓	✓					✓	
Use of personal mobile phones in the setting				✓				✓
Use of personal mobile phones in social time		✓						✓
Taking photos on personal mobile phones / cameras				✓				✓
Use of other personal mobile devices e.g. tablets, gaming devices				✓				✓
Use of personal email addresses on the setting network				✓				✓
Use of setting email for personal emails				✓				✓
Use of messaging apps		✓						✓
Use of social media				✓				✓

When using communication technologies, the setting considers the following as good practice:

- The official setting email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and children should therefore only use the setting email service to communicate with others regarding school/work related matters either when in the setting or on the setting systems (e.g. by remote access)
- Users must immediately report, to the nominated person – in accordance with the setting policy, the receipt of any communication that makes them feel uncomfortable, is

offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

- Any digital communication between staff and children or parents /carers (email, social media, chat, blogs etc) must be professional in tone and content. These communications may only take place on official (monitored) setting systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Children should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the setting website and only official email addresses should be used to identify members of staff

22. Remote Use

The school will risk assess the technology used for remote access prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The setting will ensure that all setting-owned equipment and technology used for remote access has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The setting will not be responsible for providing access to the internet off the setting premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the setting.