The Governing Body of Herons Dale have adopted the following policy

Online Safety Policy

Reviewed by: Anastasia O'Donoghue
Ratified by Governors:
Review Date: September 2023

Introduction

Herons Dale School is a Special Primary School in Shoreham which caters for pupils with a diverse range of needs, including PMLD, CLDD, SLD, MLD and ASD. We believe 'Communication is the key' to success and everything we do is geared towards developing language and communication skills.

Contents:

Herons Dale School Aims

Happy days filled with learning

A happy and relaxed child will be able to engage in all learning.

Experiences which develop a fit and healthy lifestyle

A variety of strategies and approaches in lessons along with strategic use of online content to promote health and movement will support this.

Relevant, broad, balanced, creative, and inclusive curriculums

Herons Dale teachers use a range of curriculums to ensure that all children can develop skills in all relevant areas of study supported by technology appropriate to the individual and /or group.

Opportunities to be part of the community

Pupils participate in a range of events and educational visits throughout the year, the school shares practice, news, advice and celebrations of community members online via school face book page and the school website.

Nurturing relationships

Achievements are celebrated together and where appropriate, our pupils are encouraged to work collaboratively and reflect on their learning through sharing work and experiences. Regular online safety assemblies support their understanding of positive online relationships and how to maintain personal safety.

Stimulating learning environments where pupils feel safe and secure

All learning environments are built to encourage children to develop, rehearse, consolidate, and apply their skills in a functional way with a clear understanding of why online safety rules are needed and enforced.

Diverse and personalised approaches to learning

Staff work closely with pupils to ensure learning matches their needs in the broadest possible sense, whether that be a focus on Life skills-based learning, semi-formal, hands-on approaches, or more formal techniques. Technology and access to online stimuli is carefully considered and bespoke to each group.

All-encompassing communication

Where possible, activities are supported using different communication pathways including objects of reference, symbols, PECs, pictures, eye-gaze technology, switch sounds and a multi-sensory approach. Technology is accessed through adapted screens and switches and supported with CIP.

Life skills development

Individuals and classes access appropriate accessible online safety assemblies and PSHCE content that build on their understanding of safely using tech to staying safe whilst online and what to do if they are worried.

Encouragement and support to have respect, confidence, and resilience

We always strive to ensure that pupils can reflect, recall and generalise the skills they have learnt, at a pace which supports the development of confidence, to help prepare them for their future.

Statement of intent

Herons Dale School 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 several 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, 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 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.

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 (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following school policies:

- Acceptable Use Agreement
- Data protection policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behavioural Policy
- Disciplinary Policy and Procedures
- Confidentiality Reporting Policy
- Photographic images Policy
- Mobile phone and smart device policy
- Technology Acceptable Use Agreement – Staff
- Parental use of social media policy

2. Roles and responsibilities

The governing board is 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 and throughout the year.

- Ensuring that there are appropriate filtering and monitoring systems in place.

The headteacher is responsible for:

- 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, led by the holistic provision lead, ICT coordinator and deputy DSL for online safety.
- 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.
- That the holistic provision lead supports staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- That the deputy DSL organises 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 governing board to update this policy on an annual basis.

The DSL is responsible for:

- Allocating a Deputy DSL to lead on online safety
- Ensuring identified Deputy DSL will take the lead responsibility for online safety in the school and acts as the named point of contact within the school on all online safeguarding issues.

Deputy DSL for safeguarding will be responsible for:

- 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.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up to date with current research, legislation, and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Maintain and monitor CPOMS procedure for reporting online safety incidents and inappropriate internet use by pupils.
- Establish a procedure for reporting online safety incidents and inappropriate internet use by staff.
- Ensuring all members of the school community 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 school's provision and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis via the Governors report lead by Head teacher.
- Working with the headteacher and governing board to update this policy on an annual basis.
- Be a named contact for Smoothwall monitoring service, analysing weekly reports.

TCIT technicians are 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 headteacher via Team around IT (TAIT).
- Attending half termly TAIT meetings.
- Ensuring that the school's filtering systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Reinforcing the online safety rules displayed next to every computer in class settings.
- 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 on CPOMS.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

3. 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 Identified Deputy DSL has overall responsibility for the school's approach to online safety, with support from Lead DSL and the headteacher where appropriate and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

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

- Staff receive online safety training in induction and completion of a remote access school specific course on the NATIONAL ONLINE SAFETY APP.
- Staff receive regular training updates via class meetings
- Staff receive regular email updates from National online safety App regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculums in school
- Assemblies are conducted half termly on the topic of remaining safe online. Class meetings review online safety questions set by SLT to ensure school have up to date knowledge of what pupils are accessing.

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.

Concerns regarding a staff member's online behaviour are reported to the headteacher and Lead DSL, who decides on the best course of action in line with the relevant policies, e.g., the Staff Code of Conduct and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL team via CPOMS, who investigates concerns with relevant staff members, e.g., the headteacher and TCIT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy ensuring parents are informed of the concern, action and outcome.

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

The school avoids unnecessarily criminalising pupils, 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 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 Identified Deputy DSL on CPOMs.

4. Cyberbullying

Cyberbullying can include 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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils 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.

5. 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 outside of school and off and online. They 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. Regular online safety lessons, discussions and assemblies will allow pupils the opportunity to reflect and talk. Opportunities to talk with an adult at different times will be available as pupils may not discuss or disclose in more structured timetabled sessions.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Up skirting, 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

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

6. 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, including the following. Staff will be aware the risk is greater for pupils with SEND, that access online apps and games, to be groomed and be unaware this is what is happening as:

- The pupil believes they are talking to another child, when they are talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil 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 pupil 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 pupil feel 'special', particularly if the person they are talking to is older.
- 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.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Referencing friends from online games or social media apps especially when expressing new and or concerning comments and views.
- 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 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. At Herons Dale, our more formal learners are at risk of exposure to this.

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 section of the child protection and safe-guarding 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 Prevent guidance and child-protections and safe-guarding policy.

7. Mental health

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

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. Concerns about the mental health of a pupil will be dealt with in line with the behaviour policy and Mental health Policy.

8. 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 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 Identified deputy 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.

Prior to deciding how to respond to a harmful online challenge or hoax, the Deputy DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. National Online Safety App, the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils or parents.
- 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.
- In line with the Child Protection and Safeguarding Policy.

Where the Deputy DSL's assessment finds an online challenge to be putting pupils 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 pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate. Parents will be consulted at each stage and supported to understand and work towards a solution.

The DSL and headteacher will only implement a cohort-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.

9. Online safety training for staff

The Lead and Deputy DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. Through completion of the National Online Safety training for school staff, 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.

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

10. Online safety and the curriculum

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

- RSE
- PSHE
- Computing
- Class meetings
- Class assemblies

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Engaging, semi-formal and formal cohorts access a 4-year topic cycle to ensure all elements are taught in an accessible and appropriate way. Teachers differentiate and ensure bespoke provision based on this for individuals and class groups. (See Appendix A for topic cycles and curriculum references)

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 curriculums, appropriate for each cohort, include the following:

- Rules of internet use in school
- Rules of internet use at home
- App specific input on how to safely navigate games etc online
- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculums.

The Deputy DSL is involved with the development of the school's online safety curriculum, led by the computing coordinator, and overseen by the holistic provision assistant head teacher. Pupils will be consulted on the online safety curriculum and assembly topics, 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.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff work together

to ensure the curriculum is tailored so these pupils 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. 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 pupils?
- Are they appropriate for pupils' developmental stage?

The Computing coordinator provides termly updates and guidance to ensure staff stay abreast of expectations, resources etc.

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

Before conducting a lesson or activity on online safety, the class teacher and DSL 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are 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 ensures 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. Opportunities to talk about these topics outside of the sessions will be available throughout the weeks.

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.

11. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops

- Tablets
- Internet
- Cameras
-

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 always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time and online safety rules are displayed in an accessible manner next to all computers. – this supervision is suitable to their age and ability.

12. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

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.
- 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:

- Invitation to join free membership of the National Online Safety APP
- Monthly online safety input via the school newsletter and Facebook
- 1:1 discussion
- Online resources shared on termly topic overviews
- Class or cohort updates as appropriate
-

13. Internet access

Pupils, staff, and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the school office.

All members of the school community are directed to use the school's internet network, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

14. Filtering and monitoring online activity

The governing board, supported by the Computing subject coordinator and Deputy DSL for online safety ensures the school's ICT network has appropriate filters and monitoring systems in place. TAIT (Team Around IT) ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

Filtering is monitored by TCIT services and monitoring by Smoothwall. Weekly reviews on monitoring are sent to the Deputy DSL if no concerns, which are reported on the day.

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 are appropriately monitored. All users of the network and school-owned 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 Child Protection and Safeguarding Policy.

15. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by TCIT services technicians. Firewalls are always switched on. TCIT review the firewalls on a ongoing basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments and are expected to report all malware and virus attacks to TCIT via their support email.

All members of staff have their own unique usernames and private passwords to access the school's systems. Passwords expire after 90 days, after which users are required to change them. Pupil login to a student drive only where all content is appropriate. They are unable to access the teacher or administration drive.

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 headteacher 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 the Data and Cyber-security Breach Prevention and Management Plan.

16. Emails

Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff and Volunteer Confidentiality agreement.

Staff and pupils are given approved school email accounts and are only 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 are not permitted to be used on the school internet. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

The school's monitoring system can detect inappropriate links, malware, and profanity within emails – staff and pupils are made aware of this.

Any cyber-attacks initiated through emails are managed in line with the Data and Cyber-security Breach Prevention and Management Plan.

17. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal or school use in class. Staff can use personal social media during break and lunchtimes; however, inappropriate, or excessive use of personal social media during school hours may result in further action. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to always follow these expectations.

Staff receive training on how to use social media safely and responsibly and updates and articles are shared throughout the year via shout meeting/whole school email as appropriate. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the acceptable use agreement and directed by the head teacher by a named staff member, Tracy Vise. The school's official social media channels are only used for official educational or engagement

purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent, and open to scrutiny.

18. The school website

The headteacher is 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 complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

19. Use of devices

School-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop
- Tablet
-

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets, laptops to use during lessons.

School-owned devices are used in accordance with the Device User Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

TCIT technicians review all school-owned devices on a regular basis, directed by TAIT, to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behavioural Policy respectively.

Personal devices

Personal devices are used in accordance with the Staff ICT and Electronic Devices Policy and the Pupils' Personal Electronic Devices Policy. Any personal electronic device that is brought into school is the responsibility of the user.

Personal devices are not permitted to be used in the following locations:

- Toilets
- Changing rooms

- Corridors
- Classrooms

Staff members are not permitted to use their personal devices during lesson time. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

Pupils are not permitted to use their personal devices during lesson time or when moving between lessons. If a pupil needs to contact their parents during the school day, they are allowed to use school phones. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use on such occasions as class trips and pupil transport.

Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

20. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, TCIT technicians, School business manager and the headteacher hold half termly TAIT meetings to review all aspects of online access, safety and technology

The governing board, headteacher and Deputy DSL review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is **June 2023**.

Any changes made to this policy are communicated to all members of the school community.

Appendix A:

	Summer	Autumn	
Year 1	Olympics	We can build it	
Engaging - Impacts	It functional skills impacts	It functional skills impacts	IT functional skills impacts
Semi-formal – EVOLVE / Equals / E4S	Computing basic prog HD	DL online bullying	DL internet safety and norms-
Formal - EVOLVE / Equals / E4S	Computing basic prog HD	DL online bullying	DL internet safety and norms
Year 2	Creepy Crawlies	Sights and Sounds	
Engaging - Impacts	Pmld switches equals	It functional skills impacts	It functional skills impacts
Semi-formal - EVOLVE / Equals / E4S	IT making talking books	Dl respectful relationships	It making and recording sounds
Formal - EVOLVE / Equals / E4S	IT making talking books	DL respectful relationships	IT making and recording sounds
Year 3	Move it, move it	Sparkles and shadows	
Engaging - Impacts	Making and recording sounds	It functional skills impacts	It functional skills impacts
Semi-formal - EVOLVE / Equals / E4S	Learning to control things it	DL mental wellbeing	DL being safe
Formal - EVOLVE / Equals / E4S	Learning to control things it	DL mental wellbeing	DL being safe
Year 4	Grow, Grow, Grow	Let's Go Exploring	
Engaging - Impacts	Using the computer equals	IT functional skills equals	It functional skills impacts
Semi-formal - - EVOLVE / Equals / E4S		DL health and wellbeing And lifestyle	DL self image and identity
Formal - EVOLVE / Equals / E4S	Pictograms equals it	DL health and wellbeing and lifestyle	DL self image and identity

Online Safety policy

Head Teacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher / Senior Leaders are responsible for ensuring that the staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

On Line Safety / Child Protection Lead

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- Attends relevant meeting
- Reports regularly to Senior Leadership Team
- **Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:**
- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Network Manager / Technical staff:

The Network Manager and computing Co-ordinator are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the on line safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that Atomwide is informed of issues relating to the filtering applied
- that he / she keeps up to date with e-safety technical information in order to
- effectively carry out their on-line safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse
- can be reported to the On-Line Safety Co-ordinator / Headteacher / ICT Co-ordinator for investigation / action / sanction

- that monitoring software / systems are implemented and updated as agreed in school policies
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Support for Parents

As a school we believe it is our duty to support parent and carers in keeping their child safe while using technology within the home environment. Computers and other devices in the home are more open and don't have the security features which we have in school, which does make the child more vulnerable in this environment.

The parents will be invited to On-line Safety sessions which will be held in school once a year. The school web site will have information regarding On- Line Safety for parents / carers and young people.

Although some of our pupils are unable to access the Internet some pupils are able to use the Internet independently and therefore are at risk from either deliberately accessing inappropriate material or, due to their level of literacy, accidently accessing harmful sites.
No child is able to access the Internet in school without their parents giving permission to do so. This consent form is filled in when the child starts school and is kept on record until they leave; it will only need amending if a parent/carer would like to change it.
All pupils will be taught how to use all technologies in a responsible and safe way. This will be part of the ICT curriculum.

No child may appear on the Web Site without their parent/carers consent, the consent form is completed when the child starts school and is kept on record until they leave; it will only need amending if the parent/carer would like to change it.