



School Lane, Arreton, PO30 3AD

Tel: 01983 528429

admin@arretoncepri.iow.sch.uk

Online Safety Policy

September 2025

Signed

Headteacher

Date: September 2025

Signed

Chair of Governors

Date: September 2025

Review date: September 2027

Online Safety Policy Contents

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Child-on-child sexual abuse and harassment
6. Grooming and exploitation
7. Mental health
8. Online hoaxes and harmful online challenges
9. Cyber-crime
10. Online safety training for staff
11. Online safety and the curriculum
12. Use of technology in the classroom
13. Use of smart technology
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Generative artificial intelligence (AI)
20. The school website
21. Monitoring and review

Appendices

- i) Online safety in the curriculum
- ii) Acceptable use agreement for pupils
- iii) Acceptable use agreement for staff

Statement of Intent

The Governing Body understand that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, 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 (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2025'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Responsible Internet Use Agreement
- Child Protection Policy
- Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Positive Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy

2. Roles and Responsibilities

The Governing Board will be 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 every two years or in light of any significant changes.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher will be responsible for:

- Taking the lead responsibility for online safety in the school.
- 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.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 3
--------------------	------------------------	----------------------------	------------

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DDSLs and SBM to conduct termly light-touch reviews of this policy.
- Working with the DDSLs and governing board to update this policy on biennial basis.
- 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 SBM.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure. Online safety incident for children will be recorded through CPOMs.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- 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 through Headteachers Reports.
- Working with the governing board to update this policy on a biennial basis.

ICT technician and external support will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Be aware of the child-friendly online safety policy.
- Seeking help from school 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.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 4
--------------------	------------------------	----------------------------	------------

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 Headteacher (DSL) has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

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

- Staff and governors receive regular training through the National College
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Staff receive weekly "Wake up Wednesday" online safety information
- Parents receive weekly "Wake up Wednesday" online safety information
- Online safety is integrated into learning throughout the curriculum

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 Policies.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary 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 – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. 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/DDSLs, who investigates concerns with relevant staff members, e.g. the ICT Technician and SBM, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Positive Behaviour Policy, Child Protection Policy and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher 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 Policy and Safeguarding Policy.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 5
--------------------	------------------------	----------------------------	------------

All online safety incidents and the school's response are recorded by the DSL/DDSLs.

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

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 Positive Behaviour Policy.

5. Child-on-child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

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

- 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 school culture that normalises abuse and leads to pupils 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 school 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 pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy. The child friendly child-on child abuse policy will be used with the children.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 6
--------------------	------------------------	----------------------------	------------

Concerns regarding online child-on-child abuse will be reported to the DSL/DDSLs, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policies.

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, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- 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.

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 Policies.

Radicalisation

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

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty guidelines.

7. Mental Health

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

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 7
--------------------	------------------------	----------------------------	------------

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

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

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils’ age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policies.

Where the DSL’s assessment finds an online challenge to be putting pupils at risk of harm, 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 individual pupils at risk where appropriate.

The headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils’ exposure to the risk is considered and mitigated as far as possible.

9. 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.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 8
--------------------	------------------------	----------------------------	------------

- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and ‘booting’, which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil’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 headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online Safety Training For Staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online Safety and the Curriculum

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

- Relationships and health education
- PSHE
- Computing

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

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

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

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

The DSL will be involved with the development of the school’s online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 9
--------------------	------------------------	----------------------------	------------

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher/DSL will 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 will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policies.

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 Policies.

12. Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- iPads
- Intranet
- Email
- Cameras (Including on the iPads)
- Beebots
- Microbits

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

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

Pupils will be educated on the acceptable and appropriate use of personal devices.

Staff will use all smart technology and personal technology in line with the school's Responsible Internet Use policy.

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.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Positive Behaviour Policy.

The school will cover in worship assemblies, where appropriate, any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home.

Parents will be provided with information about the school's approach to online safety and their role in protecting their children. **Parents will be sent a copy of the Acceptable Use Agreement** at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- 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 will be raised in the following ways:

- Individual Parents' meetings
- Parental information sessions delivered by a range of professionals.
- Staff training sessions
- Newsletters
- Online resources including Wake Up Wednesdays

15. Internet Access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

All members of the school community will be encouraged to use the school's internet network, instead of mobile networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering And Monitoring Online Activity

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 11
--------------------	------------------------	----------------------------	-------------

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and SBM will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate or when the technician is alerted to breaches.

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

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

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

17. Network security

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

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in Year Two and above are provided with their own unique username and private passwords.

Staff members and pupils will be responsible for keeping their passwords private.

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

Users will be required to lock access to devices and systems when they are not in use.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 12
--------------------	------------------------	----------------------------	-------------

18. Emails

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Due care and attention should be taken to understand:

- 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

19. Generative artificial intelligence (AI)

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

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school 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.

20. The school website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

21. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the headteacher/DSL, & SBM conduct regular light-touch reviews of this policy to evaluate its effectiveness.

The governing board and headteacher/ DSL will review this policy in full on a biennial basis and following any online safety incidents.

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

Appendix 1: Curriculum Coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm will be covered in the following curriculum areas: • PSHE • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm will be covered in the following curriculum areas: • PSHE • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	This risk or harm will be covered in the following curriculum areas: • PSHE
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm will be covered in the following curriculum areas: • PSHE • Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • How to report fraud, phishing attempts, suspicious websites and adverts.	This risk or harm will be covered in the following curriculum areas: • PSHE • Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas: • PSHE

	- Why passwords are important, how to keep them safe and that others might try to get people to reveal them - How to recognise phishing scams - The importance of online security to protect against viruses that are designed to gain access to password information - What to do when a password is compromised or thought to be compromised	Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as ‘harvesting’ or ‘farming’. Teaching will include the following: - How cookies work - How pupils can protect themselves and that acting quickly is essential when something happens - The rights children have with regards to their data	This risk or harm will be covered in the following curriculum areas: - PSHE - Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: - That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue - How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: - PSHE - Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following: - How to find information about privacy settings on various sites, apps, devices and platforms - That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: - PSHE - Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following: - The types of online abuse, including sexual harassment, bullying, trolling and intimidation - When online abuse can become illegal - How to respond to online abuse and how to access support - How to respond when the abuse is anonymous - The potential implications of online abuse - What acceptable and unacceptable online behaviours look like	This risk or harm will be covered in the following curriculum areas: - PSHE - Computing
Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: - How to recognise extremist behaviour and content online - Which actions could be identified as criminal activity - Techniques used for persuasion - How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following: - What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal - How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why - That it is okay to say no and to not take part in a challenge - How and where to go for help - The importance of telling an adult about challenges which include threats or secrecy, such as ‘chain letter’ style challenges	This risk or harm will be covered in the following curriculum areas: PSHE
Fake profiles	Not everyone online is who they say they are. Teaching will include the following: - That, in some cases, profiles may be people posing as someone they are not or may be ‘bots’ - How to look out for fake profiles	This risk or harm will be covered in the following curriculum areas: - PSHE - Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: - Boundaries in friendships with peers, in families, and with others - Key indicators of grooming behaviour	This risk or harm will be covered in the following curriculum areas: PSHE

	- The importance of disengaging from contact with suspected grooming and telling a trusted adult - How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following: - That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with - How to identify indicators of risk and unsafe communications - The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before - What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm will be covered in the following curriculum areas: PSHE
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following: - The issue of using image filters and digital enhancement - The role of social media influencers, including that they are paid to influence the behaviour of their followers - That 'easy money' lifestyles and offers may be too good to be true - The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm will be covered in the following curriculum areas: - PSHE - Computing
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following: - How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) - How to consider quality vs. quantity of online activity - The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out - That time spent online gives users less time to do other activities, which can lead some users to become physically inactive - The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues - That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support - Where to get help	This risk or harm will be covered in the following curriculum areas: PSHE
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: - How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure - How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm will be covered in the following curriculum areas: PSHE
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

Appendix 2: Device and Technology Acceptable Use Agreement for Pupils

At Arreton St Georges CE Primary School we know that using technology is an important part of your learning experience. We want everyone to be able to use technology, like the internet and laptops, but it is important that you are safe when you are using technology.

This agreement will set out the rules around using technology and devices, such as smart watches and phones, when you are at school. Please read this document carefully and go through it with your parent. Once you are sure that you understand the rules set out in the agreement, please sign your name, or get your parent to sign their name, at the bottom.

If you have any questions about anything in this agreement, speak to your teacher.

Definitions

Before you read the agreement, here are some key terms you should understand:

- Technology – this includes any ICT systems at the school, including the internet.
- School-owned devices – any devices that are owned by the school that have been given to you to help with your school work, including laptops and tablets.
- Personal devices – any device that belongs to you that you bring into school, including mobile phones and smart watches.

Security and protecting information

I will:

- ✓ Make sure I understand what I can do to keep my information safe when using technology and devices – I will speak to my teacher if I have any questions.

I will not:

- ✗ Try to get around any security measures the school has put in place on the internet or school-owned devices.
- ✗ Share any of my passwords with other people.

Using technology in school

I will:

- ✓ Only use technology and devices that I have been given permission to use.
- ✓ Only access websites, apps and other online platforms that I have been given permission to use.
- ✓ Only use the school's ICT facilities, technology and devices to complete schoolwork.
- ✓ Only go on the internet for something other than schoolwork during break and lunch times.

I will not:

- ✗ Install any software onto school ICT systems unless I have been told to do so by a member of school staff.
- ✗ Search for, view, download, upload or send anything inappropriate when using the internet.

School-owned devices

I will:

- ✓ Only use school-owned devices to carry out my schoolwork.
- ✓ Only use websites and apps that a member of staff has said I can use.
- ✓ Understand that the school will monitor how I use school-owned devices.
- ✓ Take care of school-owned devices when I am using them.
- ✓ Tell a member of staff if a school-owned device is damaged or lost when I am using it.
- ✓ Tell a member of staff if I think something has happened in relation to the security of the device, e.g. if I download an attachment from an email from someone I do not know.

I will not:

- ✗ Use school-owned devices to send inappropriate messages, images, videos or other content.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 17
--------------------	------------------------	----------------------------	-------------

- ✗ Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- ✗ Use school-owned devices to go on personal social media accounts.

Personal devices

If I choose to bring a personal device into school I will:

- ✓ Hand my personal device(s) into my class teacher each morning.
- ✓ Understand that if my personal devices are lost, damaged or stolen, it is not up to the school to pay for any costs.

I will not:

- ✗ Use my personal devices to send inappropriate messages, images, videos or other content.
- ✗ Use my personal devices to view, store, download or share any inappropriate, harmful or illegal content.

Reporting misuse

I will:

- ✓ Understand that my use of the internet will be monitored and recognise the consequences if I do not follow this agreement.
- ✓ Understand that the headteacher may decide to take disciplinary action against me, in accordance with the Positive Behaviour Policy, if I do not follow this agreement.

Child Agreement

I agree that I have read and understood this agreement, and ensure that I will abide by each principle.

Name	
Signature	
Date	

Parent / Carer Agreement

I agree that I have read and understood this agreement with my child, and ensure that I will encourage my child to abide by each principle and support the school in doing so

Name	
Signature	
Date	

Appendix 3: Device and technology acceptable use agreement for staff

Whilst our school promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

School computer and Internet use must be appropriate to the student's education or to staff professional activity. This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web sites, the interception of emails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the school's Data Protection Policy and any other relevant school policies and procedures.

I will not:

- ✗ Attempt to bypass any filtering, monitoring and security systems.
- ✗ Share school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so.

Using technology in school

I will:

- Follow the Staff Code of Conduct.
- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-school hours, including break and lunch time.
- Only use recommended removable media and keep this securely stored.

I will not:

- ✗ Install any software onto school ICT systems unless instructed to do so by the headteacher or SBM.
- ✗ Search for, view, download, upload or transmit any inappropriate material when using the internet.
- ✗ Visit Internet sites, make, post, download, upload or pass on material, remarks or comments that contain or relate to:-
 - Pornography (including child pornography)
 - Promoting discrimination of any kind
 - Promoting racial or religious hatred
 - Promoting illegal acts
 - Any other information that may be offensive to colleagues

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 19
--------------------	------------------------	----------------------------	-------------

Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.

I will not:

- ✗ Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- ✗ Email should be written carefully and politely, as messages may be forwarded email is best regarded a public property.

School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the headteacher.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices with me or within my sight at all times.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Seek permission from the headteacher before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors.
- Immediately report any damage or loss of my school-owned devices to the SBM.
- Immediately report any security issues, such as downloading a virus, to the SBM.
- Make arrangements to return school-owned devices to the SBM upon the end of my employment at the school.

I will not:

- ✗ Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the headteacher.
- ✗ Install any software onto school-owned devices unless instructed to do so by the headteacher or SBM.
- ✗ Use school-owned devices to send inappropriate messages, images, videos or other content.
- ✗ Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- ✗ Use school-owned devices to access personal social media accounts or public chat rooms.
- ✗ Use school-owned devices for personal gain, gambling, political purposes or advertising.

Personal devices

I will:

- Only use personal devices during out-of-school hours, including break and lunch times.
- Ensure personal devices are either switched off or set to silent mode during school hours.
- Only make or receive calls in staff only areas.
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- ✗ Use personal accounts/logins to communicate with pupils or parents.
- ✗ Access the school's Wi-Fi using a personal device unless permission to do so has been granted by the headteacher or ICT technician.
- ✗ Use personal devices to take photographs or videos of pupils or staff.

Document Ref: 3.21	Date of Issue: Sept 25	Date for Review: Sept 2027	Page No: 20
--------------------	------------------------	----------------------------	--------------------

- ✗ Store any school-related information on personal devices unless permission to do so has been given by the headteacher.

Social media and online professionalism

I will:

- Follow the school's Code of Conduct.
- Understand that I am representing the school and behave appropriately when posting on school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- ✗ Communicate with pupils or parents over personal social media accounts.
- ✗ Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- ✗ Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability.
- ✗ Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- ✗ Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- ✗ Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Working from home

I will:

- Ensure I obtain permission from the headteacher before any personal data is transferred from a school-owned device to a personal device.
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- Ensure that school work is undertaken via the Remote Log On authenticated by Duo Mobile.
- Ensure no unauthorised persons, such as family members or friends, access logons or school data.

Training

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety.
- Allow the school to undertake regular audits to identify any areas of need I may have in relation to training.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- Deliver any training to pupils as required.

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher.
- Understand that my use of the internet will be monitored and recognise the consequences if I breach the terms of this agreement.
- Understand that the headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

Agreement

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Name	
Signature	
Date	