



Online Safety Policy

At Greasley Beauvale Primary School, the Governors recognise the importance of ensuring equal opportunity for all children and adults. The Governors will continue to ensure that this is an essential element of all school policies and actions.

The right to develop, learn and work in an environment free from discrimination is implicit in our school's ethos and embodied in its Vision.

Our Vision:

At Greasley Beauvale Primary School, our vision is for everyone to **reach their true potential, nurture their talents** and foster a personal **love of learning** through a **safe, engaging and challenging curriculum**. **We take notice of each other** and **strive to be healthy and happy in body and mind**. We **champion physical, emotional and mental wellbeing** to **promote the best outcomes for everyone** to **build a healthy future together**.

At Greasley Beauvale Primary School, you are "Learning for Life" to "Paint Your Own Rainbow"

This latest update of this policy was reviewed in January 2024. The Full Governing Body approved it remotely through the SchoolBus.

Nominated staff member responsible for policy: Natasha Branigan

Next review date: Summer 2026

Signed:  (Chair)

Date: September 2025

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Peer-on-peer 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. Educating parents
14. Filtering and monitoring online activity
15. Network security
16. Social networking
17. The school website
18. Use of devices
19. Remote learning
20. Monitoring and review

Appendices

- A. Online harms and risks – curriculum coverage
- B. Flow chart for Responding to Online Safety Incidents of Misuse

Statement of intent

Greasley Beauvale Primary 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 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 members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors and community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Greasley Beauvale Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

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 (2023) 'Keeping children safe in education'
- 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'
- Counter Terrorism and Securities Act 2015

This policy operates in conjunction with the following school policies:

- School Disciplinary Procedure (Part 2) – Managing Allegations
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Employee Code of Conduct
- Behaviour Policy
- School Disciplinary Procedure (Part 1) - Managing Staff Conduct
- Prevent Duty Policy
- Peer on Peer Abuse Policy
- Blended Learning Policy
- Nurture Policy

2. Roles and responsibilities

The Governing Body 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.

- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Online Safety Governor is responsible for:

- Meeting regularly with the DSL/Online Safety Lead where collated and anonymised reports of online safety incidents will be discussed and reviewed.
- Checking that provision outlined within the Online Safety Policy is taking place (e.g. staff training).
- Ensuring that there are appropriate filtering and monitoring systems in place and review and record it's effectiveness at least annually. (The review will be conducted by members of the DLT, the DSL and the IT service provider and involve the responsible Governor - in line with DfE Filtering and Monitoring Standards).
- Reporting to relevant governors group/meetings

The headteacher / DSL 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.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- 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 Computing Leaders to conduct termly light-touch reviews of this policy.
- Working with the Governing Body to update this policy on an annual basis and reviewing the effectiveness of the filtering and monitoring system annually.
- Taking the overall responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- 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, Computing Leaders and the Online Safety Governor.
- 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.

- Being responsible for receiving reports of online safety incidents and handling them, ensuring that all incidents are recorded.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and 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 Body about online safety and providing regular reviews (anonymised) of the incidents and filtering and monitoring logs to them.

The Computing Leaders are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing and monitoring appropriate security measures as directed by the headteacher.
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.
- Monitoring and informing DSL whenever the school's filtering and monitoring system highlights a cause for concern.

ATOM ICT technicians are responsible for:

- Ensuring that the school's filtering and monitoring systems are maintained and 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.
- Understanding that online safety is a core part of safeguarding.
- Modelling safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues and of the current school Online Safety Policy and practices.
- Ensuring that learners understand and follow the Online Safety Policy and acceptable use agreements.
- Supervising and monitoring the use of digital technologies in lessons and other school activities (where allowed)
- To teach and guide learners to sites that are suitable for their use

- Having a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- 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 using CPOMs.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies on school devices and on personal devices (where allowed).
- 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.

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 school DSL has overall responsibility for the school's approach to online safety, with support from other DSL trained staff and the Computing Leaders where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. Any concerns regarding a child's online safety that are highlighted by the filtering and monitoring system will also be handled according to the relevant policies.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression.

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

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

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy and reported using the CPOMS system in school.

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, e.g. the Employee Code of Conduct, School Disciplinary Procedure (Part 2) – Managing Allegations, and School Disciplinary Procedure (Part 1) - Managing Staff Conduct. If the concern is about the headteacher, it is reported to the chair of governors. Low level concerns about a member of staff, following comments made in public about online use, may cause the headteacher to follow up informally and generally be aware of the need to be vigilant around their online use.

The filtering and monitoring system will provide reports to the DSL and Computing Leaders who will be able to see any searches that were blocked. Cause for concerns send an immediate notification to these members of staff who will then be able to investigate quickly if necessary. Where online behaviour poses a cause for concern, an investigation will take place and managed in accordance with the relevant policies and it will be recorded on CPOMS.

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

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

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

Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymised) to:

- The DSL, Headteacher, Online Safety Governor and Computing leaders for consideration of updates to policies
- Staff through briefings
- Learners through assemblies and/or lessons
- Parents/carers through newsletters, school social media, website or WEDUC
- Governors during safeguarding update meetings
- Local authority/external agencies (where relevant)

4. Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text/in app 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 media 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. Peer-on-peer sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and 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

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 Peer-on-peer Abuse Policy and the Child Protection and Safeguarding Policy.

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:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The 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.
- 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 Policy.

Radicalisation

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

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

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

Where the 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.

The DSL and 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.
- **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 consulting the Cyber Choices programme, which can help to education children at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

10. Online safety training for staff

The DSL ensures that annual safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and will be regularly updated and reinforced. 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 Anti-bullying Policy, the Peer-on-peer Abuse Policy and the Child Protection and Safeguarding Policy.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum in any lessons that use the internet to stream or search for resources. It is particularly addressed during relevant national initiatives (Safer Internet Day and Anti-bullying week) and in the following subjects:

- Computing
- PSHE
- RSE

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
- 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 curriculum. The risks that are considered and how they are covered in the curriculum can be found in [Appendix A](#) of this policy.

The school uses Purple Mash Online Safety units supplemented with learning across the curriculum and participation in nationally recognised days such as Safer Internet Day.

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, e.g. the SENCO, designated teacher for LAC and class teachers, 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?

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.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will record as an incident on CPOMS 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.

12. Use of technology in the classroom

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

- Computers, chromebooks, laptops, tablets
- Email
- 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 – this supervision is suitable to their age and ability.

13. Educating parents

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

- Monthly newsletters
- WEDUC and social media posts
- Online resources
- Periodic parents meetings

14. Filtering and monitoring online activity

The Governing Body ensures the school's ICT network has appropriate filters and monitoring systems in place that meets the standards defined in the DfE Filtering Standards for Schools and Colleges. The Governing Body ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

ATOM ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. They use their experience from support other schools in the region. The filtering and monitoring systems the school implements are 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.

Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, ATOM ICT Technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by Computing Leaders. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

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

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police and/or the LADO.

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 ATOM ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls on regularly 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 ICT technicians.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils in Year 2 and Key Stage 2 are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private.

Users inform Computing Leaders if they forget their login details, who will arrange for the user to access the systems under different login details.

16. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff are not permitted to use social media for personal use during lesson time. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Employee

Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff receive annual training on how to use social media safely and responsibly. 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, Employee Code of Conduct and Behaviour Policy.

17. The school website

The headteacher and website lead are 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 consent has been given by families.

18. 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. chromebooks or tablets to use during lessons.

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 Behaviour Policy respectively.

Personal devices

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. 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 School Disciplinary Procedure (Part 2) – Managing Allegations. 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.

Many children have mobile/smart phones which are part of their daily lives, enabling contact with parents or carers on the journey to and from school. Children in Key Stage 2 are allowed to bring mobile phones into school however these are to be turned off and stored in the teacher's desk drawer throughout the school day. As a personal possession, a mobile phone is not the responsibility of the school at any time.

Children are not permitted to bring smart watches to school due to their ability to access applications, such as social media, through connected devices (mobile phones).

Teachers have the legal right to examine any data or files on a child's mobile phone if they think there is a good reason to do so, for example (but not exclusively) if bullying or safeguarding issues are suspected. The school is not required to inform parents or carers before a search takes place or to seek their consent. Out of courtesy, the school will inform the parent or carer should such an examination take place, although this is not a requirement by law. If inappropriate or offensive material is found on the device it is up to the Head Teacher to decide whether they should delete that material or retain it as evidence for Greasley Beauvale Primary School (if a criminal offence or a breach of school discipline or whether the material is of such seriousness that it requires the involvement of the police).

19. Remote learning

All remote learning is delivered in line with the school's Blended Learning Policy.

During periods of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

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

20. Monitoring and review

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

The Governing Body, headteacher and DSL review this policy on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is Summer 2026.

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

Appendix A: Online harms and risks – curriculum coverage

[The table below contains information from the DfE’s ‘Teaching online safety in schools’ guidance about what areas of online risk schools should teach pupils about. You can use this to assist your school in developing its own online safety curriculum; however, you must develop your curriculum in line with your local needs and the needs of your pupils.]

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	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching includes the following:</p> <ul style="list-style-type: none"> • 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) 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)

<p>Disinformation, misinformation and hoaxes</p>	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 • 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 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)
<p>Fake websites and scam emails</p>	<p>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 includes the following:</p> <ul style="list-style-type: none"> • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • 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 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)

<p>Online fraud</p>	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following:</p> <ul style="list-style-type: none"> • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)
<p>Password phishing</p>	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash) • PSHE
<p>Personal data</p>	<p>Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following:</p> <ul style="list-style-type: none"> • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)

<p>Persuasive design</p>	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 • How notifications are used to pull users back online 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)
<p>Privacy settings</p>	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following:</p> <ul style="list-style-type: none"> • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)
<p>Targeting of online content</p>	<p>Much of the information seen online is a result of some form of targeting. Teaching includes the following:</p> <ul style="list-style-type: none"> • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)
<p>How to stay safe online</p>		
<p>Online abuse</p>	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following:</p>	<p>This risk or harm is covered in the following curriculum areas:</p>

	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • PSHE • Computing (Online Safety Unit – Purple Mash)
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE
Content which incites violence	<p>Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following:</p> <ul style="list-style-type: none"> • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE
Fake profiles	<p>Not everyone online is who they say they are. Teaching includes the following:</p>	<p>This risk or harm is covered in the</p>

	<ul style="list-style-type: none"> • 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 	<p>following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE • Computing (Online Safety Unit – Purple Mash)
Grooming	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following:</p> <ul style="list-style-type: none"> • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • 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 <p>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.</p>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE
Livestreaming	<p>Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following:</p> <ul style="list-style-type: none"> • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE • Computing (Online Safety Unit – Purple Mash)

	<ul style="list-style-type: none"> • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming 	
Pornography	<p>Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following:</p> <ul style="list-style-type: none"> • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE
Unsafe communication	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE

	<ul style="list-style-type: none"> • What online consent is and how to develop strategies to confidently say no to both friends and strangers online 	
Wellbeing		
Impact on confidence (including body confidence)	<p>Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 • The issue of photo manipulation, including why people do it and how to look out for it 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE
Impact on quality of life, physical and mental health and relationships	<p>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 includes the following:</p> <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • PSHE

<p>Online vs. offline behaviours</p>	<p>People can often behave differently online to how they would act face to face. Teaching includes the following:</p> <ul style="list-style-type: none"> • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • PSHE
<p>Reputational damage</p>	<p>What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following:</p> <ul style="list-style-type: none"> • Strategies for positive use • How to build a professional online profile 	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> • Computing (Online Safety Unit – Purple Mash)
<p>Suicide, self-harm and eating disorders</p>	<p>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.</p>	<ul style="list-style-type: none"> • PSHE

Appendix B: Responding to Online Safety Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

