

Widney Junior School



Online Safety Policy

Revision Date: September 2026

Review Date: September 2027

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. Social networking
 21. The school website
 22. Use of devices
 23. Remote learning
 24. Monitoring and review
-

Appendix

[Appendix 1: Consent form for pupils/parents and covering letter](#)

[Appendix 2: Responsible Internet and E-mail use: Agreement for parents](#)

[Appendix 3: Widney guidelines for responsible internet use for children](#)

[Appendix 4: Acceptable Use Policy](#)

[Appendix 5: Staff Internet Access Agreement](#)

[Appendix 6: SMART rules for safe internet use \(from Childnet International\)](#)

[Appendix 7: Online harms and risks – curriculum coverage](#)

[Appendix 8: Online Safety Long Term Plan](#)

[Appendix 9: Responding to incidents of misuse](#)

[Appendix 10: Pupil Acceptable Use Agreement](#)

Statement of intent

Widney Junior 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 Online Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Bullying, PSHE and Child Protection.

This Policy was written in line with Solihull MBC Policy Guidance which itself incorporates elements of good practice from Kent and Warwickshire. The policy also uses information shared on the SWGfL website which focuses specifically on online safety and the effects of a digital footprint.

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 (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence 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'
- 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:

- Social Media Policy
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Home Learning 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 on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and 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:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and School ICT Support Officer to conduct annual light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO, Computing lead and School ICT Support Officer.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.

- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher, Computing Lead and School ICT Support Officer to conduct annually light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

School ICT Support Officer 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.
- Working with the DSL and headteacher to conduct annual light-touch reviews of this policy.

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.
- 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 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
- A planned online safety curriculum is provided as part of Computing / PHSE / Assemblies / other lessons and are regularly revisited.
- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils safe use of technology is also monitored by Smoothwall, to monitor the use of technology and any incidents are reported to the DSL in keeping children safe online.
- The 'Big Red Button' has been installed on pupil laptop computers in the computing suite. Pupils use this button to report inappropriate content.
- Staff receive regular email updates and CPD meetings 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 half-termly on the topic of remaining safe online by the Computing lead

Handling online safety concerns

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

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

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary 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, who investigates concerns with relevant staff members, e.g. the headteacher, School ICT Support Officer, Computing lead, 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.

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 Anti-Bullying Policy.

5. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur 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 and the Social Media Policy.

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. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with 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, 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 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 Safeguarding Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

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

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 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 Social, Emotional and Mental Health (SEMH) 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, 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 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 a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and 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
- Half-termly Assemblies by Computing Lead
- 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 3](#) 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, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

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

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

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and 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 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 will be used during lessons, including the following:

- Computers
- Laptops
- iPads
- Intranet
- Email
- Cameras (iPads)

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 and will use technology in line with the school's Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the school's Staff ICT and Electronic Devices Policy.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate 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 Behaviour Policy.

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

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

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

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 also have access to current and up-to-date information about apps and websites which can be found on the school's website.

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:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources

- School website with information about Online Safety

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. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

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 School ICT Support Officer 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. School ICT Support Officer will undertake weekly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

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

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

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

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

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

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

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in year 3 and above are provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will inform School ICT Support Officer or the Computing lead 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.

Any suspected cyber security breach must be reported immediately to the Headteacher and Computing Lead.

18. Emails

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

Staff 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 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 School ICT Support Officer. 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. Computing lead will organise an annual assembly where they explain what a phishing email and other malicious emails might look like – this assembly will include information on the following:

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

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

19. Generative Artificial Intelligence (AI)

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

The school will ensure its IT systems include appropriate filtering and monitoring systems to limit pupils' ability to access, generate or share harmful, inappropriate or unsafe content through generative AI tools.

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

The school will take steps to ensure that personal, confidential and sensitive information is not entered into generative AI tools and that individuals cannot be identified through information submitted to such systems.

The school will make use of current guidance and support to establish a safe, secure and reliable foundation before adopting new and emerging AI technologies.

The school will teach pupils to critically evaluate information, images, videos and other content generated by AI, recognising that AI-generated content may be inaccurate, biased, misleading or entirely fabricated.

Pupils will be educated about the risks associated with deepfakes, manipulated media and synthetic content, including how such technologies may be used to spread misinformation, commit fraud, facilitate bullying or damage reputations.

Where AI tools are used to support teaching and learning, staff will ensure that pupils understand when AI has been used to generate content and will promote appropriate attribution, honesty and academic integrity.

Staff using AI tools for educational or administrative purposes will do so in accordance with the school's data protection, information security and safeguarding procedures and will exercise professional judgement when reviewing AI-generated outputs.

The school will regularly review emerging developments in AI technology, associated risks and national guidance to ensure that its safeguarding, online safety and data protection arrangements remain effective and up to date.

Any concerns relating to the misuse of AI, including the creation or sharing of harmful, inappropriate, deceptive or abusive AI-generated content, will be managed in line with the school's safeguarding, behaviour and anti-bullying procedures.

20. Social networking

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

21. 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.

The website will be managed in line with the School Website Policy.

22. Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff ICT and Electronic Devices Policy.

23. Remote learning

All remote learning will be delivered in line with the school's Home-Learning Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

24. Monitoring and review

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

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

The next scheduled review date for this policy is **September 2027**

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

Widney Junior School

Online Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Pupil:

Class:

Pupil's Agreement

- I have read and I understand the school Online Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed (Pupil):

Date:

Parent/Carer's Consent for Web Publication of Work and Photographs

- I agree that my son/daughter's work may be electronically published.
- I also agree that appropriate images and video that include my son/daughter may be published, subject to the school rule that photographs will not be accompanied by pupil names.

Parent/Carer's Consent for Internet Access

- I have read and understood the school Online safety rules and give permission for my son/daughter to access the Internet.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
- I understand that the school cannot be held responsible for the content of materials accessed through the Internet.
- I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed (Parent/Carer):

Date:

Please print name:

Appendix 2: Responsible Internet and E-mail use: Agreement for parents

Please complete, sign and return to the school as soon as possible.



WIDNEY JUNIOR SCHOOL

Inspiring a community

Respect, Kindness, Determination, Collaboration, Responsibility, Honesty

Head Teacher: Mrs J Bridges BA (QTS) NPQH

Clifton Crescent, SOLIHULL, West Midlands B91 3LQ
Tel: 0121 -705-8516 Fax: 0121-709-1005

Email: office@widney.solihull.sch.uk Web: www.widney.solihull.sch.uk Twitter: @WidneyJS

Dear Parent

Responsible Internet and E-mail use: Parental Agreement

As part of the National Curriculum Information and Communications Technology programme, children are able to have supervised access to the internet and e-mail. This area of our work is now considered within the framework of safeguarding children and the school has produced a Policy for Online safety which outlines our approach to ensuring that children learn how to use ICT safety.

With this letter you have been given a copy of our Guidelines for Responsible Internet use and a form to complete. We are required to ask you to sign the form as a way of giving your consent for your child to use the ICT facilities as part of their learning.

Both you and your child should sign the form and return it to the school as soon as possible.

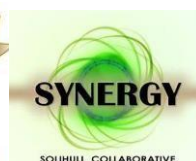
The educational benefits of internet and e-mail access have been made very clear as they allow pupils to explore and evaluate a wide range of information sources and to communicate and collaborate with other learners around the world. All of this work is closely supervised in the school and procedures and

technological structures are in place to minimise any risk of children accessing inappropriate material. The Council network incorporates a filtering system and the children's curriculum includes a programme of learning about safe and appropriate behaviours to adopt when using ICT.

During school, teachers will guide children towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio. The school will provide guidance materials for families when appropriate and a Workshop for parents will hopefully take place early in the Summer term. Look out for details.

Yours sincerely,

Mrs J Bridges



Appendix 3: Widney guidelines for responsible internet use for children

Guidelines for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These guidelines will keep everyone safe and help us be fair to others:

I will use only my own login and password, which I will keep private.

I will not access other people's files.

I will use the computers only for school work.

I will not bring memory sticks or CDs into school to use without permission.

I will ensure I have permission from a member of staff before using a computer.

I will only e-mail people I know, or my teacher has approved.

The messages I send will be polite and sensible.

I will not give my home address, phone number or other details about myself, or arrange to meet someone.

I will turn off the screen and tell a teacher if I see anything I am unhappy with or I receive a message I do not like.

I will only visit websites or carry out Internet searches that my teacher has approved.

I understand that the school can check my computer files and the Internet sites I visit.

[Appendix 4: Acceptable Use Policy](#)

Acceptable Internet Use Policy

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head Teacher and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / extranet / network, or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will only use the approved *office email to communicate* with parents/carers, and only communicate with them on appropriate school business.
- I will not use school or personal email to communicate at all with any pupils.
- I will not browse, download or send material that could be considered offensive or inappropriate to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the head teacher.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software.
- If I use any personal device (e.g. home laptop, tablet, mobile phone), I will ensure that this is password protected and not accessed by anyone else.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the shared drive within school.
- I will not use a personal mobile device at school anywhere where children are present and it will remain switched off during lesson time.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to contain no mention of the school and are not confused with my professional role.

- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.
- I will only access school resources remotely (such as from home) using the Solgrid remote access portal and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff at the school.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the head teacher on their request.
- I understand that Internet encrypted content (via the https protocol), will be scanned for security and/or safeguarding purposes.
- I will take responsibility for logging and ensuring actions are taken following an online safety incident.
- *Staff that have a teaching role only:* I will embed the school's online safety curriculum into my teaching.

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature Date
 Full Name (printed)
 Job title / Role

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature Date

Full Name (printed)

[Appendix 5: Staff Internet Access Agreement](#)

Widney Junior School

Widney Junior School – Online safety Policy

Responsible Internet use – Staff consent form

As a member of staff at Widney Junior School, I have read the Online Safety Policy and Guidelines for Responsible Internet Use.

I agree to abide by the Policy in all aspects of my professional role and will only use internet access in a manner appropriate to my position.

I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damage arising from use of the internet.

Signed:
Please print name:
Date:
Please return the signed form to the school office.

Appendix 6: SMART rules for safe internet use (from Childnet International)



The infographic features a red background with various icons and text boxes. At the top, a green banner reads 'Be smart on the internet' with a yellow pushpin. To the right is a laptop and a smartphone. In the top right corner is the Childnet International logo and website address. The five SMART rules are presented in colored boxes with corresponding icons: a padlock for 'SAFE', two people for 'MEETING', a folder for 'ACCEPTING', a question mark for 'RELIABLE', and a speech bubble for 'TELL'. The bottom section includes the KidSMART logo, the website 'www.kidsmart.org.uk', and a cartoon character pointing towards the text.

Be smart on the internet

Childnet International
www.childnet.com

S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the Internet may not be true, or someone online may be lying about who they are.

t TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk

THINK UK KNOW

www.kidsmart.org.uk

KidSMART Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Appendix 7: Online harms and risks – 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 • Computing
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 • 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	This risk or harm will be covered in the following curriculum areas: • PSHE • Computing

	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	
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 - How to identify 'money mule' schemes and recruiters - The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal - The risk of sharing personal information that could be used by fraudsters - That children are sometimes targeted to access adults' data - What 'good' companies will and will not do when it comes to personal details - 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: - 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	This risk or harm will be covered in the following curriculum areas: - PSHE - 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 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	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

Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following: • 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	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	All areas of the curriculum

	• Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	
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 • Computing
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following: • 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	This risk or harm will be covered in the following curriculum areas: • PSHE • Computing
Fake profiles	Not everyone online is who they say they are. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	• 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	• 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 • 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.	This risk or harm will be covered in the following curriculum areas: • PSHE • Computing
Livestreaming	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 will include the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • 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	This risk or harm will be covered in the following curriculum areas: • PSHE • Computing

	• 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	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching will include the following: • 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, e.g. revenge porn or people trafficked into sex work	This risk or harm will be covered in the following curriculum areas: • PSHE • Online Safety lessons
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 • Computing

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
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	This risk or harm will be covered in the following curriculum areas: • Relationships and Health education • PSHE

	• Where to get help	
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: • Online Safety • Relationships education • Computing
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following: • Strategies for positive use • How to build a professional online profile	This risk or harm will be covered in the following curriculum areas: • Online Safety • Computing • 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.	This risk or harm will be covered in the following curriculum areas: • Online Safety • Computing • PSHE

Appendix 8: Online Safety Long Term Plan

Widney Junior School – Online Safety Long Term Plan



The united curriculum for computing and online safety is built upon:

- Computing: The 'Purple Mash' Curriculum
- Online Safety: Education for a Connected World, Jigsaw, Project Evolve and BBC OWN IT resources

Online Safety objectives are integral to the Computing and PSHE curriculum. We will:

- Adapt some lessons in the Purple Mash / PSHE Jigsaw units using resources from Project Evolve and BBC Own IT.
- Teach an online safety lesson as the **first lesson** in Computing for each year group from year 3 to year 6.
- Weekly in-class assemblies to promote online safety across the school.
- Half-termly assemblies delivered by Computing subject leader with updates.

Children are provided with:

- ✓ Relevant, coherent, progressive computing education that equips them to use computational thinking and creativity.
- ✓ Computer science - The principles of information and computation, how digital systems work, and how to put this knowledge to use through programming.
- ✓ Opportunities to create programs, systems and a range of content.
- ✓ Opportunities to express themselves and develop their ideas through, information and communication technology at a level suitable for the future workplace and as active participants in a digital world.
- ✓ A comprehensive curriculum for online safety to ensure the messages around online safety are reinforced throughout the year including assemblies, Internet Safety Day and Anti-bullying week.

WHOLE SCHOOL OVERVIEW 2023-2024

	YEAR 3	YEAR 4	YEAR 5	YEAR 6
Autumn 1	Manage online information	Manage online information	Manage online information	Manage online information
Autumn 2	Online bullying	Online bullying	Online bullying	Online bullying

Spring 1	Online Reputation	Online Reputation	Online Reputation	Online Reputation
Spring 2	Health, Well-being and lifestyle	Health, Well-being and lifestyle	Health, Well-being and lifestyle	Health, Well-being and lifestyle
Summer 1	Online relationships	Online relationships	Online relationships	Online relationships
Summer 2	Self-image and identity	Self-image and identity	Self-image and identity	Self-image and identity

The titles of topics have been taken from the objectives of Education for a connected world.

Year 3: Online Safety Long Term plan

To be taught as the first computing lesson of each half-term.

TERM	Lesson Focus	PSHE Link	Project Evolve Success Criteria	Weekly Class Discussion	Assemblies
Autumn 1	Managing online information		LEP: I can explain that not all opinions shared may be accepted as true or fair by others. Year 3\Autumn 1 - Managing online information	1. Binge watching 2. Loot boxes 3. Internet Hack 4. Avoiding account hacks 5. Nailing Online Safety	Privacy and security
Autumn 2	Online bullying	Jigsaw – Puzzle 2 Celebrating Differences Puzzle 5 Relationships (Piece 3)	LEP: I can describe appropriate ways to behave towards other people online and why this is important Year 3\Autumn 2 - Online Bullying	1. 7 tips to beat cyberbullying 2. 5 things to ask 3. Anonymous bullying 4. Why do people bully? 5. How to tell if your friend needs help	Anti-Bullying Week 13.11.23
Spring 1	Online Reputation	Jigsaw – Puzzle 5 Relationships (Piece 3)	LEP: I can explain how to search for information about others online Year 3\Spring 1 - Online Reputation	1. Social Media 2. Oversharing information 3. Digital footprint 4. 5 ways for a better internet 5. Positive online reputation	Internet Safety Day
Spring 2	Health, well-being and lifestyle	Jigsaw – Puzzle 4 Healthy Me	LEP: I can explain why spending too much time using technology can sometimes have a negative impact on anyone. Year 3\Spring 2 - Health, well-being and lifestyle	1. Do you spend too much time online? 2. Why is it so bad to us? 3. Take a breath 4. Vlogger 5. Symptoms online	Health, well-being and lifestyle
Summer 1	Online Relationships	Jigsaw –Puzzle 5 Relationships	LEP: I can explain what it means to ‘know someone’ online and why this might be different from knowing someone offline. Year 3\Summer 1 - Online Relationships	1. top tips 2. I’m a MEME 3. Top tips for staying connected 4. Supporting your friends online 5. Girl gamer 6. Selfies	Online Relationships

Summer 2	Self-image and identity	<u>Jigsaw –</u> <u>Puzzle 2</u> Celebrating Difference	LEP: I can explain what is meant by the term ‘identity.’ Year 3\Summer 2 - Self-image and identity	Online scams Online gaming Digital consent Living your life online Identity theft Gaming profiles	Self-image and identity
----------	-------------------------	---	---	--	-------------------------

Year 4: Online Safety Long Term plan

To be taught as the first computing lesson of each half-term.

TERM	Lesson Focus	PSHE Link	Project Evolve Success Criteria	Weekly Class Discussion	Assemblies
Autumn 1	Managing information online		LEP: I can describe how to search for information within a wide group of technologies and make a judgement about the probable accuracy. Year 4\Autumn 1 - Managing information online	1. Binge watching 2. Loot boxes 3. Internet Hack 4. Avoiding account hacks 5. Nailing Online Safety	Privacy and security
Autumn 2	Online bullying	Jigsaw – Puzzle 2 Celebrating Difference	LEP: I can describe ways people can be bullied through a range of media (e.g. image, video, text, chat.) Year 4\Autumn 2 - Online Bullying	1. 7 tips to beat cyberbullying 2. 5 things to ask 3. Anonymous bullying 4. Why do people bully? 5. How to tell if your friend needs help	Anti-Bullying Week 13.11.23
Spring 1	Online Reputation		LEP: I can describe how to find out information about others by searching online Year 4\Spring 1 - Online Reputation	1. Social Media 2. Oversharing information 3. Digital footprint 4. 5 ways for a better internet 5. Positive online reputation	Internet Safety Day
Spring 2	Health, well-being and lifestyle	Jigsaw – Puzzle 4 Healthy Me	LEP: I can explain how using technology can be a distraction from other things, in both a positive and negative way. Year 4\Spring 2 - Health, well-being and lifestyle	1. Do you spend too much time online? 2. Why is it so bad? 3. Take a breath 4. Vlogger 5. Symptoms online	Health, well-being and lifestyle
Summer 1	Online Relationships	Jigsaw –Puzzle 5 Relationships	LEP: I can give examples of how to be respectful to others online and describe how to recognise healthy and unhealthy online behaviours Year 4\Summer 1 - Online Relationships	1. 5 top tips 2. I'm a MEME 3. Top tips for staying connected 4. Supporting your friends online 5. Girl gamer 6. Selfies	Online Relationships

Summer 2	Self-image and identity	Jigsaw – Relationships (Piece 1)	LEP: I can describe positive ways for someone to interact with others online and understand how this will positively impact on how others perceive them. Year 4\Summer 2 - Self-image and identity	1. Online scams 2. Online gaming 3. Digital consent 4. Living your life online 5. Identity theft 6. Gaming profiles	Self-image and identity
----------	-------------------------	---	---	--	-------------------------

Year 5: Online Safety Long Term plan

To be taught as the first computing lesson of each half-term.

TERM	Lesson	PSHE Link	Project Evolve Success Criteria	Weekly Class Discussion	Assemblies
Autumn 1	Managing online information	<u>Jigsaw – Puzzle 5</u> Relationships (Pieces 2-6)	LEP: I can explain the benefits and limitations of using different types of search technologies. E.g. voice-activation search engine. Year 5\Autumn 1 - Managing information online	1. Binge watching 2. Loot boxes 3. Internet Hack 4. Avoiding account hacks 5. Nailing Online Safety	Privacy and security
Autumn 2	Online bullying	<u>Jigsaw – Puzzle 2</u> Celebrating Differences <u>Puzzle 5</u> Relationships (Piece 2)	LEP: I can describe how what one person perceives as playful joking and teasing (including 'banter') might be experienced by others as bullying Year 5\Autumn 2 - Online Bullying	1. 7 tips to beat cyberbullying 2. 5 things to ask 3. Anonymous bullying 4. Why do people bully? 5. How to tell if your friend needs help	Anti-Bullying Week 13.11.23
Spring 1	Online Reputation	<u>Jigsaw – Puzzle 5</u> Relationships (Pieces 2-6)	LEP: I can search for information about an individual online and summarise the information found. Year 5\Spring 1 - Online Reputation	1. Social Media 2. Oversharing information 3. Digital footprint 4. 5 ways for a better internet 5. Positive online reputation	Internet Safety Day
Spring 2	Health and well-being and lifestyle	<u>Jigsaw – Puzzle 4</u> Healthy Me <u>Puzzle 5</u> Relationships (Piece 5)	LEP: I can describe some strategies, tips or advice to promote health and well-being with regards to technology Year 5\Spring 2 - Health, well-being and lifestyle	1. Do you spend too much time online? 2. Why is it so bad to us? 3. Take a breath 4. Vlogger 5. Symptoms online	Health and well-being and lifestyle
Summer 1	Online Relationships	<u>Jigsaw - Puzzle 5</u> Relationships (Piece 2-6)	LEP: I can explain that there are some people I communicate with online who may want to do me or my friends harm.	1. 5 top tips 2. I'm a MEME 3. Top tips for staying connected 4. Supporting your friends online 5. Girl gamer	Online Relationships

			Year 5\Summer 1 - Online Relationships	6. Selfies	
Summer 2	Self-image and identity	Jigsaw – Relationships (Piece 1)	LEP: I can demonstrate how to make responsible choices about having an online identity, depending on context. Year 5\Summer 2 - Self-image and identity	1. Online scams 2. Online gaming 3. Digital consent 4. Living your life online 5. Identity theft 6. Gaming profiles	Self-image and identity

Year 6: **Online Safety** Long Term plan

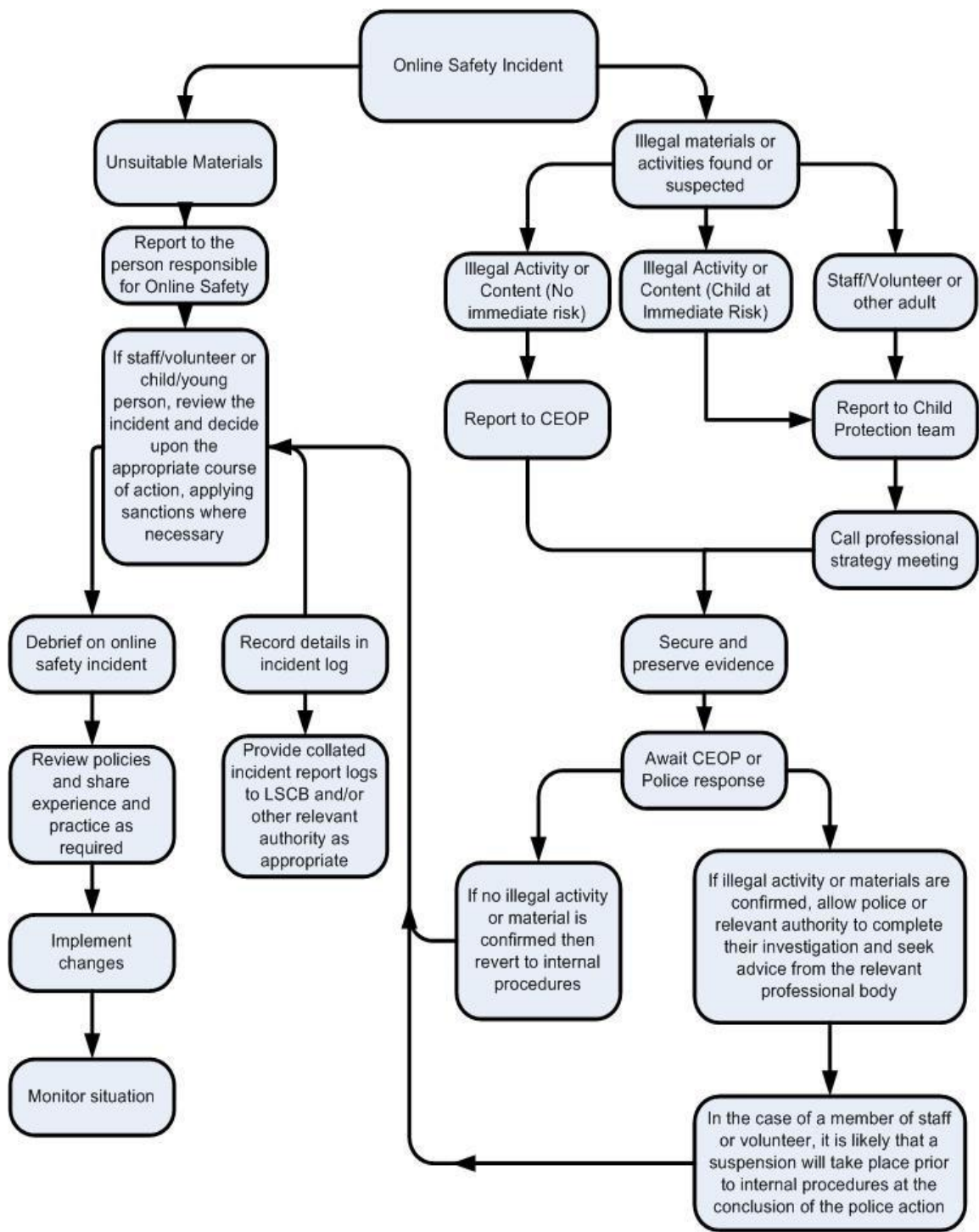
To be taught as the first computing lesson of each half-term.

TERM	Lesson Focus	PSHE Link	Project Evolve Success Criteria	Weekly Class Discussion	Assemblies
Autumn 1	Managing online information	Jigsaw – Puzzle 5 Relationships (Piece 5)	LEP: I can define the terms ‘influence’, ‘manipulation’ and ‘persuasion’ and explain how someone might encounter these online (e.g. advertising and ‘ad targeting’ and targeting for fake news) Year 6\Autumn 1 - Managing information online\I can define the terms influence	1. Binge watching 2. Loot boxes 3. Internet Hack 4. Avoiding account hacks 5. Nailing Online Safety	Privacy and security
Autumn 2	Online bullying	Jigsaw – Puzzle 1 Celebrating difference (Piece 4)	LEP: I can explain how someone would report online bullying in different contexts Year 6\Autumn 2 - Online Bullying\I can explain how someone would	1. 7 tips to beat cyberbullying 2. 5 things to ask 3. Anonymous bullying 4. Why do people bully? 5. How to tell if your friend needs help	Anti-Bullying Week 13.11.23
Spring 1	Online Reputation	Jigsaw – Puzzle 5 Relationships (Piece 6)	LEP: I can explain the ways in which anyone can develop a positive online reputation Year 6\Spring 1 - Online Reputation\I can explain the ways in which	1. Social Media 2. Oversharing information 3. Digital footprint 4. 5 ways for a better internet 5. Positive online reputation	Internet Safety Day
Spring 2	Health and well-being and lifestyle	Jigsaw – Puzzle 4 Healthy Me	LEP: I can describe common systems that regulate age-related content (e.g. PEGI, BBFC, parental warnings) and describe their purpose. Year 6\Spring 2 - Health, well-being and lifestyle\Health Well being and Lifestyle\I can describe common systems th	1. Do you spend too much time online? 2. Why is it so bad to us? 3. Take a breath 4. Vlogger 5. Symptoms online	Health and well-being and lifestyle
Summer 1	Online Relationships	Jigsaw – Puzzle 1 Being me in my world Puzzle 5 Relationships (Piece 5&6)	LEP: I can describe how things shared privately online can have unintended consequences for others. e.g. screen-grabs. Year 6\Summer 1 - Online Relationships\Online Relationships\I can describe how things shared	1. 5 top tips 2. I’m a MEME 3. Top tips for staying connected 4. Supporting your friends online 5. Girl gamer 6. Selfies	Online Relationships

Summer 2	Self-image and identity	<u>Jigsaw – Puzzle 5</u> Relationships	LEP: I can describe issues online that could make anyone feel sad, worried, uncomfortable or frightened. I know and can give examples of how to get help, both on and offline. Year 6\Summer 2 - Self-image and identity\Self Image and Identity\I can describe issues online tha	Online scams Online gaming Digital consent Living your life online Identity theft Gaming profiles	Self-image and identity

Appendix 9: Responding to incidents of misuse

– flow chart



Appendix 10: Pupil Acceptable Use Agreement



Pupil Acceptable Use Agreement

When using technology for learning...	
• I will only access computing equipment when a trusted adult has given me permission and is present. • I will not deliberately look for, save or send anything that could make others upset. • I will immediately inform an adult if I see something that worries me, or I know is inappropriate. • I will keep my username and password secure; this includes not sharing it with others. • I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names. • I will always use my own username and password to access the school network, Century, Purple Mash, TT Rockstars and Spelling Shed and any other programmes the school uses. • In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me. • I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.	• I will use all communication tools such as email, Class Dojo and Zoom carefully. I will tell an adult immediately if I notice that someone who is not approved by the teacher is messaging. • I will always dress appropriately for live lessons and behave sensibly, just like I am expected to in my normal classroom. • Before I share, post or reply to anything online, I will T.H.I.N.K. T = is it true? H = is it helpful? I = is it inspiring? N = is it necessary? K = is it kind?

I understand this agreement and know it is important that I follow the rules for my safety and the safety of others.

My name	
My parent's signature	

My class	
Date	