CARWARDEN HOUSE COMMUNITY SCHOOL

Online Safety Policy

Adopted:	October 2024
Due for review:	September 2025
Author:	ICT Lead
Approved by:	Headteacher

Policy Statement & Aims

Carwarden House Community School recognises the importance of technology and the Internet to our students' lives and their learning. The Internet is an essential element in 21st century life for education, business and social interaction and it offers unimaginable opportunities and is constantly evolving. Using ICT to interact socially, to learn independently and to share positive ideas is beneficial to everyone, but it is essential that students, staff and parents understand the potential dangers and use this technology safely.

This policy refers to the safe use of the Internet, but it also covers the use of mobile phones and other electronic communication devices. We know that some adults and young people will use these technologies to harm children. This harm might range from sending hurtful or abusive texts and emails, to encouraging children to engage in sexually harmful conversations or actions online, (e.g. creating or sharing indecent photos / videos, inappropriate webcam activity or arranging potentially harmful face-to-face meetings).

The school has a 'duty of care' and responsibility to educate all members of the school community on the risks and responsibilities of online safety. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to safely regulate ICT activity within school and to provide a good understanding of appropriate ICT use so that members of the school community can ensure their online conduct is safe for themselves and others.

Online safety is a whole-school issue and responsibility.

This policy should be read in conjunction with the following policies:

- Safeguarding and Child Protection
- Anti-Bullying
- Behaviour
- Staff Code of Conduct and Student Acceptable Use Policy.
- SRE and PSHE
- Data Protection/GDPR

1. Roles and Responsibilities

The ICT Lead is: **Louise Treumann** who acts as school online safety coordinator.

The designated member of the board of Trustees responsible for online safety is:
Carol Blunden-Lee.

Trustees

The role of the designated online safety Trustee will include:

- To ensure an online safety policy is in place, it is reviewed every year and is available to all.
- To ensure that there is an online safety coordinator who has been appropriately trained and able to effectively lead on online safety in the specific context of our school.
- To ensure that procedures for the safe use of ICT and the Internet are in place, understood by all and consistently adhered to.
- To hold the Headteacher and staff accountable for all aspects of online safety.

Headteacher and DSL

The Headteacher and the DSL have responsibility for ensuring the safety (including online safety) of all members of the school community. Any complaint about staff misuse must be referred to a DSL, or in the case of a complaint about the Headteacher, to the Chair of Trustees. The Headteacher will:

- Ensure access to induction and training in online safety practices for all users.
- Ensure all staff receive regular update training.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet 'filtering' methods are appropriate and effective.
- Ensure that staff or external providers who operate monitoring systems are appropriately supervised and accountable.
- Ensure that student or staff personal data recorded within the school information management system and shared using the Internet is secure and in compliance with GDPR requirements.
- Work with the Internet Service Provider, Zen Zero and school ICT Manager to ensure systems to protect students are effective, appropriate and managed correctly (in line with DfE guidance and requirements).
- Ensure the school ICT system and network is reviewed regularly in relation to cyber security, that all known risks are ameliorated, and that virus protection is installed and updated as required.
- The Senior Leadership Team will receive half-termly monitoring reports from the online safety coordinator.

ICT Lead who acts as Online safety coordinator

- Develops, liaises with SLT on the online safety induction and training updates for staff & students.
- Liaises with SLT, the Internet Service Provider, school IT technical services and school systems to ensure systems to protect students are regularly reviewed and remain effective.
- Receives brief reports of online safety incidents from DSL/SLT to help inform future online safety developments.
- Liaises with the designated member of the Board of Trustees and the Headteacher to be aware of the annual report on online safety.

IT Management / Technical Support (outsourced currently to Zen Zero):

The IT Management providers are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / virtual learning platform / remote access and email is continuously monitored in order that any misuse / attempted misuse can be reported to the Headteacher / DSL for investigation & action.

That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and all Classroom Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices
- They report any suspected misuse or problem to the Headteacher or SLT
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- Ensure online safety issues are embedded in all aspects of the curriculum
- Ensure students understand and follow the student friendly online safety policy
- Monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. (Smooth wall has been put in place).

Parents / Carers Are responsible for ensuring that:

- Digital and video images taken at school events aren't shared online
- They are aware and able to access the parents' sections of the website / Remote Education/(SeeSaw)
- Their children's personal devices in school are the responsibility of the child/ren

Communicating School Policy

This policy is available from the school office and on the school website for parents, staff, and students to access. Online safety guidelines are displayed around the school. Online safety should be integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons or Connections time where personal safety, responsibility, and/or development are being discussed.

2. Making use of ICT and the Internet in school

The internet is used in school to support students learning, to raise educational standards, to promote student achievement, and to support the professional work of staff and the school's management functions. Technology is advancing rapidly and is now a significant part of everyday life, education and business. We believe our students need to be able to understand and confidently / safely use technology to be active and healthy participants in society and to prepare them for adulthood and employment.

Some of the benefits of using ICT and the Internet in schools are:

For students:

- Access to learning whenever and wherever convenient.
- Range of accessible resources matched to the needs of the learner.
- The ability to individually tailor accessibility to their learning needs.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within the safety of a classroom.
- Access to a wide range of media to enhance understanding.
- Individualised access to learning.
- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Access to subject experts, role models, inspirational people and organisations. The Internet can provide a great opportunity for students to interact with people that they otherwise would
- never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration (locally, nationally, and globally); self-evaluation; feedback and assessment; updates on current affairs as they happen.

For staff:

- Professional development opportunities
- Immediate professional and personal support through networks, forums and associations.
- Improved access to technical support.
- Ability to set individualised learning activities for and interact with students who are required to learn at home.
- Ability to provide immediate feedback to students and parents.
- Class management, reporting safeguarding concerns, attendance records, schedules, and assignment tracking. (Track-It, CPOMS, SIMS, Solar),
- Supporting lesson planning and subject development

For parents:

- The ability to speedily and conveniently contact staff, raise queries or receive information.
- Being able to see the work their child has done or is doing.
- To be able to receive regular advice and resources on how they can better support their child's learning at home (e.g. monitor homework tasks).
- Access for their child to recommended learning platforms and resources.
- Ability to share their child's successes outside school (e.g. photos of achievements and significant events).
- Easy and immediate access to school information, policies and updates.
- Ability to use secure systems for school related payments (e.g. SCOPAY).
- Speedy access to surveys and requests for information (including consents).

3. Learning to Evaluate Internet Content

With so much information available online it is important that students learn how to evaluate Internet content for accuracy and intent. This is taught by the school as part of online safety across all subjects in the curriculum. Students are taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- Acknowledge the source of information used and to respect copyright.
- To understand the consequences of copying somebody else's work in an exam or a piece of coursework and that they may be prohibited from completing that exam.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable or inappropriate sites, then they should report the URL to the DSL and online safety coordinator. All Internet use in monitored remotely by 'Smooth wall' and a daily report sent to the DSL who will take action as required. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies by the DSL. Continuous software and broadband checks take place to ensure that filtering services are working effectively (Barracuda- email filtering).

4. Managing Information Systems

The school is responsible for reviewing and managing the security of our computers and associated networks and takes the protection of school data and personal protection of our school community very seriously (complying in full with GDPR requirements). This includes protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The IT Management providers review the security of the school information systems and users continuously and virus protection software is updated regularly. They report any issues and resolutions to the DSL.

Examples of safeguarding tools that the school uses to secure our computer systems are Smooth wall Web Filtering for students and Barracuda Networks Email Security. The school ensures that:

- All personal data sent over the Internet (or taken off site) is encrypted.
- Staff only use approved school email accounts for work related matters.
- That unapproved software/apps are not downloaded to any school devices.
- Files held on the school network will be regularly checked for viruses by ZenZero.
- The use of user logins and passwords to access the school network are mandatory.
- Portable media containing school data or programmes are not taken off-site without specific permission from a member of the senior leadership team and this is logged.

For more information on data protection in school please refer to our **Data Retention/Protection Policy**. More information on protecting personal data can be found in **section 11** of this policy.

5. Emails

The school uses email to communicate internally with staff and students, and externally with parents, other professionals and suppliers / contractors, and is an essential part of school communication. Email is also used to enhance the curriculum by:

- Initiating contact and sharing learning plans & resources with each other and with the wider staff team.
- Providing opportunities for learning when preparing students for adulthood, further education and employment.
- Providing immediate feedback on work and responding to requests for support where it is needed.

The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

School Email Accounts and Appropriate Use

Staff should be aware of the following when using email in school:

- Staff should only use official school provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are always representing the school and should take this into account when entering into any email communications.
- Staff must immediately inform a member of the senior leadership team if they receive any offensive, threatening or unsuitable email on their school account either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of 'chain messages' is not permitted in school.
- To comply with GDPR regulations, staff should not share confidential personal email addresses with any third party (e.g. any email to more than one parent should be sent individually or using 'bcc').

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In school, students should only use school provided email accounts
- Students should immediately tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Students must not reveal any personal information in email or arrange to meet up with anyone who they have met online without specific permission from an appropriate adult.

Students will be educated through the ICT curriculum to help them to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

6. Published Content and the School Website

The school website is viewed as an essential tool for communicating our school ethos, values and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up to date with school news and events, celebrating whole-school and individual student achievements, and promoting school projects.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the school will be for the school office or specific staff only (e.g. DSL). **For information on the school policy on children's photographs on the school website please refer to section 7.1 of this policy.**

Our School website and Facebook page are updated and maintained on a regular basis. These are both monitored by the Trustees.

6.1 Policy and Guidance of Safe Use of Student's Photographs and Work

Photographs and students work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the General Data Protection Regulation 2018 images of students and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. For students 13 and above their explicit consent is also required. The school does this to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used
- How long parents are consenting the use of the images for
- School policy on the storage and deletion of photographs.

6.2 Using photographs of individual students

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or undertaking school activities without the school's permission. The school follows general rules on the use of photographs of individual children.

- Parents and others attending school events can take photographs and videos of their own children at those events and only for domestic purposes. The school does not, however, agree to any such photographs or videos being used for any other purpose (e.g. shared with others than immediate family).
- The school asks that parents and others do not post any images or videos which include any student other than their own child on any social media or otherwise publish those

images or videos.

As a school we want to celebrate the achievements of our students and therefore may want to use images and videos of our students within promotional materials, or for publication in the media such newspapers covering school events or achievements. We will seek the consent of students, and their parents where appropriate, before allowing the use of images or videos of students for such purposes.

6.3 Complaints of Misuse of Photographs or Video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any complaints will be dealt with in line with the school's **Child Protection & Safeguarding** policy and **Behaviour Policy.** Misuse of photographs or videos in any form will be dealt with in accordance with the school behaviour policy relevant to the incident type.

6.4 Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social media sites (Snapchat, X, Instagram), bulletin boards, chat rooms and instant messaging/WhatsApp. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are potentially more vulnerable to content and potentially harmful contact. We seek to educate all students so that they can make their own informed decisions and take responsibility for their conduct online. Students are not allowed to access social media sites in school and there are restrictions on the use of these sites in school that apply to staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT and PSHE Curriculum about the risks and responsibility of sharing personal information and the difficulty of 'taking it down' completely once it is out in such a public place.

- Students are educated on the potential dangers of social networking sites and how to use them in safe and positive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and acceptable online behaviour.
- Any site that is to be used in a class activity is risk-assessed by the teacher prior to the lesson to ensure that the site is age-appropriate and entirely safe for use.
- Students are encouraged not to publish specific and detailed private thoughts, views or ideas that might be considered hurtful, harmful or defamatory on social media.

7 Mobile Phones and Personal Device

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them is important for the school. Some issues surrounding the possession of these devices are they:

- Can make students more vulnerable to cyberbullying
- Can be used to access inappropriate internet material
- Can be a distraction in the classroom

- Are valuable items that could be stolen, damaged, or lost
- Often have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school:

- Mobile phones of students in KS3 & KS4 are handed in at morning registration and stored securely by staff until they are returned at the end of the day.
- 6th Form students are permitted to keep their phones on them during the day but their use is tightly monitored by staff.
- Staff are not permitted to use personal phones during the working day unless given specific permission by SLT.

The school does not tolerate cyber-bullying. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of this type will be disciplined.

SLT can confiscate a student's mobile phone if it has not been handed in or it is deemed the student may have used it inappropriately. Further, a member of SLT can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.

- Mobile phones must be switched off and handed in in the morning to be stored safely away until the end of the school day.
- Any student who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in school.
- If staff wish students to use these devices in class as part of a learning activity, they must get permission from a member of the senior leadership team and guidance from online safety lead.

Mobile Phone or Personal Device Misuse

Students

- Students who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.
- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being prohibited from taking that exam.

8 Cyberbullying

The school, as with any other form of bullying, takes Cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in

the **behaviour policy and the school anti-bullying policy.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to students what is expected of them in terms of respecting their peers, staff and members of the public, and any intentional breach of this will result in disciplinary action.

A young person may be reluctant to speak out about abuse they've experienced online. They may:

- not understand that they are being abused
- feel dirty and/or ashamed or feel it is their fault
- be too embarrassed to share the details of what has happened to them (particularly if it is of a sexual nature)
- be afraid because of threats of violence from the abuser
- have been told by the abuser that they won't be taken seriously or believed
- have established an emotional attachment with the abuser and don't want to get them into trouble

If an allegation of cyber bullying is made, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider to identify the bully or view harmful material.
- Record and report the incident (using CPOMS).
- Provide support and reassurance
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as. a group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

Any sanction used will be appropriate and proportionate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

The school has a child protection policy and procedures (available on our website) that sets out what action staff and volunteers should take if they have concerns about a child's safety online.

9 Everyone who works or volunteers for our school is required to read and understand these documents. Managing Emerging Technologies

Technology is progressing rapidly, and new technologies are emerging all the time. The School will risk-assess any new technologies before they are allowed in school and will consider any educational benefits that they might have. The school attempts to keep up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

10 Protecting Personal Data

Carwarden House School believes that protecting the privacy of our staff and students and

regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect, and process is used correctly and only as is necessary, and the school will keep parents fully informed of how data is collected & stored, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school community to ensure that we are doing all we can to support both staff and students.

In line with the General Data Protection Regulation 2018, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection **read the school's data protection policy on our website.**

This policy will be reviewed annually by the ICT Lead and approved by the Headteacher.

Useful Websites with further information:

Resources for professionals:

NSPCC Helpline: www.nspcc.org.uk/keeping-children-safe/reporting-abuse/nspcc-helpline

The UK Safer Internet Centre: https://swgfl.org.uk/services/professionals-onlinesafety-helpline

Helpline number: 0844 381 4772 or email: helpline@saferinternet.org.uk

Internet Watch Foundation: reporting page - https://www.iwf.org.uk/report

Resources for parents:

NSPCC Keeping Children safe online

Parental Controls How to set up controls on devices.

CEOP Education Information for parents and carers to help protect for children and young people from online sexual abuse.

Staying safe online | Childline

Reporting

If you think a child is in immediate danger, contact the police on **999**. If you're worried about a child but they are not in immediate danger, you should share your concerns.

- **Follow the school safeguarding and child protection policy guidelines available on our website.**
- Contact the NSPCC Helpline on **0808 800 5000** or by emailing **help@nspcc.org.uk.** Their trained professionals will talk through your concerns with you and give you expert advice.
- For families living in Surrey, c**ontact your local child protection service** at **cspa@surrey.gov.uk** or phone 0300 470 9100. If you live outside Surrey your Local Authority will have alternative contact details.

If your concern is about online sexual abuse, you can make a report to the

Child Exploitation and Online Protection (CEOP) command