Parrs Wood High School

E-Safety Policy

effective from 28th November 2018

(This policy supersedes all previous performance management policies adopted by or in use by the Governing Body)

Formatted: Width: 21 cm, Height: 29.7 cm

Approval History

Approved By:	Date of Approval	Version Approved	Comments
LGB	January 2017	1	

Revision History

Revision Date	Previous Revision Date	Rev	Summary of Changes	Changes Marked	Owner/Editor
Nov 18	Jan 17	1	On document highlighted	y	

Content Page

Policy Implementation

- The school has appointed E–Safety Coordinators – Mr A ~~Chalmers~~ Cumbor, ~~and~~ Mrs V Moloney and the safeguarding lead Mrs J Barrens
- The E–Safety Policy and its implementation will be reviewed annually.
- Our E–Safety Policy has been written by the school, building on government guidance.
- Parrs Wood High School Policy has been agreed by the Senior Leadership Team and approved by governors.

1. Managing Information Systems

1.1 How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly by ~~Capita~~ ICT technicians and Mrs C Wright (designated SLT link)~~.~~
- Virus protection will be updated regularly, this is done automatically by ~~Capita~~ICT technicians.
- Unapproved software will not be allowed in work areas or attached to email – ~~Capita~~ICT technicians has set a no permission setting on this.
- Files held on the school's network will be regularly checked through regular virus scans.
- The ICT coordinator/network manager will review system capacity regularly (Mr A ~~Chalmers~~Cumbor).

1.2 How will email be managed?

- Students may only use approved email accounts for school purposes.
- Students must immediately tell a designated member of staff if they receive offensive email. This will then be dealt with following the guidelines of the anti-bullying policy.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team.

1.3 How will published content be managed?

- The contact details on the website should be the school address and telephone number. Staff or students' personal information must not be published.
- The school website and SIMS Learning Gateway will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

1.4 Can students' images or work be published?

- Images or videos that include students will be selected carefully.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Students sign a consent form at the start of the year giving them the option to allow / not allow for their images to be published on the school website.

1.5 How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites using appropriate filtering settings controlled by ~~Capita~~ICT technicians~~.~~Network administrator A Cumbor
- Students will be advised never to give out personal details of any kind which may identify them and/or their location. This is reinforced during curriculum time spent on E-Safety.
- Staff wishing to use Social Media tools with students as part of the curriculum will assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- Staff official blogs or wikis should be password protected and run from the school website.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of the E-Safety training. Safe and professional behaviour will be outlined in the school Acceptable Use Policy which is signed at the start of every year.

1.6 How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of students. This is maintained and controlled by ~~Capita~~ICT technicians.
- The filtering policy will be reviewed on a regular basis by ~~Capita~~ICT technicians.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) will be aware of this procedure which will be highlighted in the E-Safety training and be part of the Acceptable Use Policy.
- If staff or students discover unsuitable sites, the URL will be reported to the School E-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

1.7 How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed, this will be decided by the Director of ICT Faculty and Mrs C Wright.
- Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Agreement.

1.8 How is classroom technology behaviour managed?

- All classrooms are provided with a behaviour management system (Netsupport) that monitors students' behaviour and progress on the computers.

- Staff are trained in the use of Netsupport as part of the E-Safety training. They can carefully monitor the online activity of students and automatically ban students if there is any inappropriate behaviour.
- Sanctions following the schools behaviour policy are followed if students fail to adhere to the classroom rules of computer use. These include the suspension of students' accounts.

2. Policy Decisions

2.1 How will Internet access be authorised?

- All staff will read and sign the 'School ICT Acceptable Use Policy' before using any school ICT resources.
- Parents will be asked to read the School ICT Acceptable Use Policy for student access at the start of each school year and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy
- ~~The school operates through a managed service controlled by Capita~~, ~~they~~ The ICT technicians have secure firewall and security policies in place to ensure safety on the internet.
- The school has the right to view and monitor any data on the network, including email and internet usage.

2.2 How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

2.3 How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, cyber bullying, illegal content etc.). This is covered via the E-Safety curriculum and the school website.
- The E-Safety Coordinator will record all reported incidents and actions taken via the SIMS Learning Gateway.
- The Designated Child Protection ~~Coordinator~~ Officer J Barrens will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage E-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.

2.4 How will E–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.

- Any complaint about staff misuse will be referred to the head teacher.
- All E–Safety complaints and incidents will be recorded by the school, including any actions taken.

2.5 How will Cyber bullying be managed?

- Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of Cyber bullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyber bullying following the school's behaviour policy.
- Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's E-Safety ethos.

2.6 How will Learning Platforms (Eg. Google classrooms) be managed?

- SLT and ~~Capita~~ICT technicians will regularly monitor the usage of the LP by students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current student, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, students etc. leave the school their account or rights to specific school areas will be disabled.

2.7 How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices must be switched off when on the school site.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if it is being used. The phone or device might be searched by the Senior Leadership Team.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- If a student breaches the school policy then the phone or device will be confiscated and will be held in a safe in the appropriate Key Stage office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

3. Communication Policy

3.1 How will the policy be introduced to students?

- All users will be informed that network and Internet use will be monitored.
- An E–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst students.
- Student instruction regarding responsible and safe use will be detailed in the AUP.

3.2 How will the policy be discussed with staff?

- The E–Safety Policy will be formally provided to and discussed with all members of staff.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school.

3.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school E–Safety Policy in newsletters, the school prospectus and on the school website.
- Information and guidance for parents on E–Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents. This can be found on the school website.

4. Delivery of E-Safety

4.1 How will E-safety be delivered to students?

- Students are taught the topic of E-Safety in discrete ICT lessons, which covers how to stay safe both at school and home.
- E-Safety issues are also covered within the Personal Development Curriculum throughout all Key Stages.
- The curriculum is continually updated to ensure all advances in technologies are covered and up to date. This will be monitored by the Director of ICT Faculty.
- Appropriate E-Safety themed assemblies based on the Stay Safe issues will be delivered to all Key Stages on an annual basis. There will be a different theme each year.

4.2 How will students learn how to evaluate Internet content?

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Schools E-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection ~~Coordinator~~Officer, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the school an e-Safety Policy?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. students, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, students and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Is e-Safety training provided for all students (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	Y/N
Do parents/carers or students sign an Acceptable Use Policy?	Y/N

Are staff, students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N
Does the school log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	