The Parkside School
learn grow thrive

Parkside E-safety Policy

Approved by:	C. Ellis-Gage
Signed:	
Next review due:	September 2023
by:	

Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk, especially those with special educational needs, within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers.
- Risk of Criminal exploitation e.g. county lines/Incel culture/radicalisation
- Cyber-bullying/ peer on peer abuse / inappropriate social development
- Access to unsuitable video / internet games

The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying). It is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build our pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. This policy supports this by identifying the risks and the steps we are taking to avoid them.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk as stated within Keeping Children Safe in Education:

1. Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
2. Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
3. Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

4. Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

(DfE Keeping Children Safe in Education 2021)

Development and Monitoring
Computing Co-ordinator David Hook
Designated Safeguarding Lead : John Habershon

This e-safety policy has been developed by the Computing Co-ordinator and the Designated Safeguarding Lead in conjunction with the School Leadership team. As part of this policy, records will be maintained of E-Safety related incidents involving staff and pupils and any incidents recorded will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

Roles and Responsibilities
Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness.

The Computing Co-ordinator + Designated Safeguarding Leads:
• Are responsible for the implementation and effectiveness of this policy. They are also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
• Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
• Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
• Report any serious breaches of the E-Safety Policies
• Provide training and advice for staff
• Liaise with the Local Authority where necessary
• Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
• Are trained in and shares with staff awareness and understanding of e-safety issues and the potential for serious child protection issues that can arise.

Teaching and Support Staff
Teaching and Support Staff are responsible for ensuring that:
• They have an up to date awareness of e-safety matters and of the current school e safety policy.
• They have read, understood and signed the E–Safety policy, school Staff Acceptable Use Policy / Agreement (AUP)
• They report any suspected misuse or problem to a designated Safeguarding Lead for investigation. (CPOMS)

• Digital communications with pupils and parents / carers (email) are on a professional level

Pupils

- Pupils understand and follow the Parkside computer use rules and, where possible, school e-safety policy
- Pupils know how they can report abuse, misuse or inappropriate materials
- Understand that the school's E-Safety Policy covers their actions out of school, if related to another pupil, where appropriate for age and ability.

Education – Pupils

E-Safety education will be provided in the following ways, as appropriate to pupils' age and ability:

• The school's e-safety curriculum is integrated as part of Computing/ PHSE / RSE as well as other lessons.

• Key e-safety messages are continually reinforced throughout the school.

• Staff act as good role models in their use of ICT, the internet and mobile devices

• Pupils are allowed to search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites that are visited. Filters are in place to ensure pupils can only access appropriate content.

Education - Parents

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. The school will therefore seek to provide information and awareness to parents and carers through:

• Letters, emails and through the school website

• Reference to external E-Safety websites

• Online learning opportunities

Acceptable use of the internet in school

- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- If necessary the school can monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- Parkside uses securely, a cloud-based web-filtering system, across the school to provide a safe internet environment for staff and students alike. Securly helps deliver the appropriate filtering to each user. Securly can produce activity logs to designated staff across the school for some of the more serious activity that require further investigation.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are **not** permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Staff may ask to see a pupil's mobile device to support any ongoing e-safety issues. Staff have the right to retain mobile phones, or other online technologies, if there is deemed to be a justifiable safeguarding risk.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends