Parklands High School
An Academy

Online Safety Policy

Parklands High School

November 2022

Next Review; November 2023

Version 202223.NF/AD.v1

Online Safety Policy

Rationale

At Parklands High School we acknowledge that digital technologies are integral to the lives of young people both within and outside of school. The internet and other technologies are powerful tools which open up new opportunities. All young people have an entitlement to access such technologies in order to enhance motivation and engagement, and thus facilitate continued improvements in standards across all curriculum areas. The requirement to ensure that young people are able to use technologies appropriately, and safely, should be addressed as part of the wider duty of care to which all those who work in schools are bound. This online safety policy should ensure safe and appropriate use of technology. The implementation of this strategy involves all stakeholders in the school community.

Purpose

This policy addresses the potential risks associated with using the online technologies, including:

- Access to illegal, harmful or inappropriate images, harmful websites and unsuitable video/internet games.
- The risk of being subject to grooming via the internet, and possibly meeting high risk individuals in person.
- The sharing and/or distribution of personal images without the individual's consent or knowledge.
- Inappropriate communication with others, including strangers.
- Cyber bullying.
- Illegal downloading of files.
- The inability to evaluate the accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement and unauthorised access to, or loss of, or inappropriate sharing of personal information.
- The risk of becoming involved in extremist groups or 'radicalised' (Prevent Duty).

School Aims

- To have processes in place to ensure the online safety of pupils and staff.
- To deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The three key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as child-to-child 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
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools.
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff.
- Relationships and sex education.
- Searching, screening and confiscation.

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

The Governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will coordinate regular meetings with appropriate staff to discuss online safety.

All governors will:

- Ensure that they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children.

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL, Mrs Fairhurst, are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes the lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, Network Manager, and other staff as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing body.

Network Manager

The school Network Manager is responsible for:

- Putting in place an appropriate level of security procedures, such as web filtering systems, which are monitored and updated regularly.
- Ensure that the school's ICT systems are secure and protected against viruses and malware.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyberbullying are flagged to the DSL and dealt with appropriately in line with the school behaviour policy.

Staff

All staff, including agency staff and volunteers, are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on the Staff Acceptable Use policy, and ensuring that students follow the Pupil Acceptable Use policy.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately, in line with this policy.

Parents

Parents are expected to:

- Notify a member of staff if they have any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms of the Pupil Acceptable Use policy.

Parents can seek further guidance on Keeping Children Safe online from the following organisations and website:

- UK Safer Internet Centre - https://saferinternet.org.uk/guide-and-resource/
- Childnet Advice - https://www.childnet.com/help-and-advice/parents-and-carers
- Child Exploitation and Online Protection - https://www.ceop.police.uk/Safety-Centre/
- Get Safe Online - https://www.getsafeonline.org/

Educating Pupils about online safety

Pupils will be taught about online safety as part of the curriculum. This will include:

- Understanding how to use technology safely, respectfully, responsibly, and securely.
- Recognising inappropriate content, contact, and conduct, and how to report concerns.
- Learning about online risks, including that any material someone provides to another, has the potential to be shared online. Also, the difficulty of removing potentially compromising material placed online.
- The impact of viewing, or sharing, harmful content.
- How to identify harmful behaviours online, and how to report it.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children.

Educating Parents about Online Safety

The school aims to raise parents' awareness of internet safety via communications home and information shared via the school's website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised with the DSL.

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.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them in class, unless given permission from a member of staff.

Any breach of the Acceptable Use Policy agreement by a pupil may trigger disciplinary action in line with the school's behaviour policy, which may result in the confiscation of their device.

Should a pupil use a mobile phone, in school, without express permission from a member of staff, it will be confiscated, placed in the office and returned at the end of the day.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyberbullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example, through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages.
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
    - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by the appropriate Houseleader or, if necessary, a member of the Senior Leadership Team.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school's safeguarding procedures.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues relating to online safety.

This policy will be reviewed every year.

At every review the policy will be shared with the school governors.

This policy should be read in conjunction with the Behaviour, Safeguarding and Code of Conduct policies.