OVERSTONE PARK SCHOOL

E-Safety (Digital Resilience) Policy

JUNE 2024
OVERSTONE PARK SCHOOL
Overstone Park, Northampton, NN6 0DT

E-Safety (Digital Resilience)

Date	Review Date	Coordinator
June 2024	September 2024	Mrs M Brown - Principal Mrs D York – DSL Miss A West – DSL Ms J Sinnamon – Deputy DSL

Overstone Park School recognises that e-safety is a safeguarding and child protection matter.

The School Governing body (The proprietors) and the DSL have overall strategic responsibility for filtering and monitoring, supported by the school's IT specialists and IT consultant.

The school:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems.
- Review filtering and monitoring provision regularly (at least termly).
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

At Overstone Park School we use a system which prevents access to inappropriate websites, provides alerts on detected student safety issues and monitors student wellness levels.

It should be noted that technical monitoring systems do not stop unsafe activities on a device or online. Staff and volunteers must remain vigilant and ensure they are physically monitoring pupils where possible. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example:

pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

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.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, 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, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The policy applies to all School pupils, staff, and the wider school community and should be read in conjunction with other relevant school policies including:

- ICT & Mobile Phone Acceptable Use Policy (for staff and pupils).
- Safeguarding and Child Protection Policy.
- Staff Code of Conduct.
- Data Protection Policy.
- Social media policy.
- Code of Conduct for remote learning.
- Policy to Counter Bullying.
- Rewards and Sanctions Policy.

All of these policies can be found on the school website.

This policy covers:

Anyone logging into any network, service, website or portal associated with Overstone Park School.

Connecting a device via the Overstone Park School network.

Any electronic communication with an Overstone Park School pupil, member of staff or contractor from any geographic location both on site and off site.

The school encourages pupils to use new technologies for their important educational and social benefits. This policy aims to balance the desirability of fully exploiting this potential with providing safeguards against risks and unacceptable materials and activities.

Our approach is to implement safeguards within the school and to support staff and pupils to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance, and the implementation of our associated policies.

This policy covers both technologies provided by the school and those owned by pupils and staff but brought onto school premises. Although pupils may be trusted by their parents with regard to private internet use, the school has a legal obligation to safeguard all pupils.

The internet provides a range of social media tools that allow users to interact with one another, share news and events and build communities around shared mutual interests.

While recognising the benefits of social networks, this policy sets out the principles that pupils, staff and the wider school community are expected to follow when using social media and the internet.

E-safety and safeguarding issues are dealt with by the Safeguarding Team, in line with the School's Child Protection Policy. In furtherance of our duty to safeguard pupils and protect them from the risk posed by extremism and radicalisation, we will do all that we can to make our pupils and staff stay safe online and to satisfy our wider duty of care.

Concerns regarding cyber-bullying can be reported to any member of staff, then, in accordance with the School's Policy to Counter Bullying, this should be reported to the pupil's mentor who will then consult with the Deputy DSL or a member of the DSL team as appropriate. The concerns will then be dealt with in line with the Child Protection and Rewards and Sanctions policy accordingly.

Our Aims:

Pupils are keen to grasp the opportunities offered by new technology and the availability, portability, miniaturisation and sophistication of electronic devices. However, there are associated risks which include the following: exposure to inappropriate material, physical danger, cyber-bullying, radicalisation, legal and commercial issues, gambling and addictive behaviour.

Overstone Park School seeks to promote a culture of digital resilience. This helps individuals recognise and manage the risks they come across when they socialise, explore or work online.

We educate our pupils, parents and staff about how to behave responsibly and protect themselves online.

The school aims to protect and safeguard pupils in their use of technology by:

Ensuring that all pupils are IT literate and can use the facilities so that their education provision is enhanced to the maximum. Raising awareness and countering instances of cyber-bullying.

Cyber-bullying is when the Internet, mobile phones or other devices are used to send or post text or images intended to hurt or embarrass another person. It may also include threats, sexual remarks, pejorative labels (i.e. hate speech), ganging up on victims by making them the subject of ridicule in forums, and posting false statements as fact aimed at humiliation.

Raising awareness and building resilience to radicalisation, through PSHE sessions and communication with parents, in combination with filtered internet access.

Enabling appropriate and careful use of social networking sites or personal web pages.

Responsibilities

The reporting responsibilities for e-safety follow the same lines of responsibility as safeguarding.

All Staff:

- ✓ Are responsible for ensuring the safety of all pupils.
- ✓ Must report any concerns or disclosures to a DSL or the Senior Deputy as appropriate in a timely fashion.

- ✓ Must never offer assurance of confidentiality.
- ✓ Must keep to the terms and conditions of the ICT Acceptable Use Policy at all times
- ✓ Must attend staff training on e-safety.
- ✓ Must actively promote good e-safety practice.
- ✓ Must communicate with pupils professionally and in line with the Staff Code of Conduct.

All Pupils:

- ✓ Must keep to the terms and conditions of the ICT Acceptable Use Policy at all times.
- ✓ Must receive appropriate e-safety guidance as part of their programme of study.
- ✓ Should inform a member of staff if they are worried or concerned an e-safety incident has taken place involving them or another member of the school community.
- ✓ Pupils must act safely and responsibly at all times when using the internet and/or mobile technologies.

The DSL:

The Designated Safeguarding Lead has responsibility for understanding the filtering and monitoring systems and processes in place. At Overstone Park school we use Fortigate to support filtering and monitoring of internet use.

- ✓ Must refer to appropriate additional support from external agencies.
- ✓ Must call e-safety meetings when required.
- ✓ Must ensure the delivery of staff training using their own expertise or calling on appropriate providers.
- ✓ Must record e-safety safeguarding incidents.
- ✓ Must report any developments in patterns and concerns to the SLT. Must liaise with the local authority and external agencies to promote e-safety within the school community.

IT Department:

- ✓ Must ensure the School's IT infrastructure is secure and meets best practice recommendations.
- ✓ Must ensure IT security incidents are recorded, reported, investigated and resolved within a reasonable timescale. Must report any e-safety concerns or disclosures immediately to a DSL.

<u>Procedures and Practices</u>

The school provides every pupil with internet access and access to the school network. The following measures are in place to protect the safety and interests of all pupils and staff and inhibit abuses:

The Use of Technology - pupils are not required to have mobile phones in school and should use them only in accordance with the School's Mobile Phone Policy, during the day. Students have access to school computers and are permitted to bring their own laptop devices. Visitors to the site may be given a time-limited code, providing access to a restricted WiFi network, where necessary. All visitors are subject to the terms of the Visitors Policy.

ICT & Mobile Phone Acceptable Use Policies for Staff and Pupils

These protect all parties by clearly stating what is acceptable and what is not, with regard to the use of technology in the classroom and beyond.

Keeping the School Network Safe:

All users have their own private username and password and are advised not to be careless or negligent with their passwords.

All network activity is logged.

Pupils must not attempt to bypass the school's network or system security by installing or configuring VPN, proxies, web anonymisers or any other solution designed to bypass web filtering and/or provide anonymous access to the internet.

The IT department monitors email traffic and blocks SPAM and certain attachments. The school has strong anti-virus protection on its network which is operated by the IT department.

Staff Training - Staff are trained, as part of their professional development, in online safety and safeguarding matters such as the Prevent Duty.

Web Filtering

Filter includes the ability to generate instant alerts for blocked content, the DSL and the IT team configure filtering settings to allow for different alert levels for vulnerable users to scan documents, emails, chats, images, and videos for inappropriate content. Students trying to access unsuitable material will be blocked, an alert generated and the activity logged against the student. The DSL and their team will then investigate via the reporting system.

Web Monitoring - The School exercises the right to monitor the use of computer systems including monitoring of internet use, interception of emails and the deletion of inappropriate materials at all times.

The system monitors search, web browsing, and web based social media, email, documents, drives, messaging, in Google and Microsoft environments.

Using AI, the system identifies and categorises harmful activity. The system generates real time alerts which are sent to the DSL team. Where an alert indicates a significant and immediate concern, an email is sent to the DSL team and a member of SLT allowing them to respond.

Management of Data - The personal data of staff, students and parents is held and processed by the school, in accordance with statutory requirements and in line with the School's Data Protection Policy.

The school reserves the right to request to see the contents of any removable device that is, or is suspected to have been, connected to the school's network.

Parental Engagement

The School gives guidance to parents/carers covering online safety and digital resilience. The purpose of these sessions is to create a shared understanding between staff, pupils and parents with regard to e-safety issues. Emails are sent to parents and guardians highlighting key issues in cyberbullying, e-safety and the use of social media.

Overstone Park Expectations of Pupils and Parents outside of the School

Overstone Park School expects the use of technology by its students, even when at home, to comply with the school's ethos and to honour the agreement permitting the use of ICT at school.

Material downloaded in the home, posted on the internet using a home computer or transmitted to a mobile phone when a pupil is not at school, can impact significantly upon the lives of pupils and other members of the school community.

Pupils should be aware that computer/mobile phone, emails and social network sites may be scrutinised for the purposes of safeguarding or promoting a child's welfare or maintaining and promoting the wellbeing of the school community as a whole.

Behaviour and Sanctions

Where conduct is found to be unacceptable, the school will deal with the matter internally and refer to relevant policies, for example the behaviour policy.

Where conduct is considered illegal, the school will report the matter to the police.

Safeguarding and Remote education:

Guidance to support schools and colleges understand how to help keep pupils, students and staff safe whilst learning remotely can be found at Safeguarding and remote education - GOV.UK (www.gov.uk) and providing remote education: guidance for schools - GOV.UK (www.gov.uk). The NSPCC also provides helpful advice - Undertaking remote teaching safely.

Overstone Park is in in regular contact with parents and carers.

We use communication to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online. (Refer to remote education policy)

Monitoring and Review

The working of this Policy will be monitored locally by the Designated Safeguarding Lead in the School who will report as required to the Principal.

The Proprietor of the school, the Designated Safeguarding Lead and a Safeguarding Consultant will undertake an annual audit visit and other periodic checks in order to monitor the effectiveness of the school's implementation of these policies and procedures, together with regular reviews of the safeguarding incidents that have arisen and how they were managed.

The Health and Safety management team will also participate in the process of reviewing the policy.

Principal:	**Mrs M Brown**	**Date:**	**June 2024**