HIGHFIELDS SCHOOL

ONLINE SAFETY POLICY

BOUNDARY WAY, PENN, WOLVERHAMPTON, WV4 4NT
Telephone: 01902 556530 Fax: 01902 556531 E-mail: enquiries@hswv.co.uk Website: www.hswv.co.uk

At Highfields School we have

- Robust processes in place to ensure the online safety of students, staff, volunteers and Governors/Trustees
- An effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Established clear mechanisms to identify, intervene and escalate an incident, where appropriate

Roles and responsibilities

The Local Governing Board

The Local Governing Board has overall responsibility for monitoring this policy and has delegated responsibility for implementation to the Headteacher.

The Local Governing Board will receive regular briefings from the Designated Safeguarding Lead (DSL) and Child Exploitation Online Protection (CEOP) Ambassador to receive updates relating to online safety at Highfields School.

All Governors and Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

The Headteacher

The Headteacher is responsible for ensuring consistent and school-wide implementation of this policy

The Designated Safeguarding Lead (DSL)

Details of the school's DSL and Deputies are set out in the Safeguarding Policy. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring school-wide implementation of this policy.
- Working with the Headteacher, Strategic Infrastructure Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents and reports of cyberbullying are logged and dealt with appropriately in line with this policy and the school's 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 Local Governing Board

The Strategic Infrastructure Manager is responsible for:

- Establishing appropriate filtering and monitoring systems, which will keep students safe from potentially harmful, dangerous and inappropriate or harmful content or contact while at school.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- Ensuring that any online safety incidents and reports of cyberbullying are logged and dealt with appropriately in line with this policy and the school's Behaviour Policy.
- Training all staff and educating students, staff and Governors/Trustees regarding CEOP.

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

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use
- Reporting immediately any online safety incidents or reports of cyberbullying

Student Devices
All students at Highfields are provided with a Windows laptop. The devices have been invaluable in aiding with schoolwork, both in class and at home. This scheme has allowed the school to innovate in the ways we have been able to deliver our curriculum through Office 365 and Show My Homework and is an effective means of supporting students with preparations for their GCSE and school exams.

The devices allow access to Microsoft Office applications at school and home. Students and parents/carers have access to the Show My Homework site which establishes links between home and school. Each device has an antivirus software programme and will notify ICT Services of any unauthorised activity at school or home. A parent/carer Laptop Agreement is entered into before the device is issued.

Any use of personal mobile devices in school by students must be in line with the Mobile Phone Policy.

Filtering and Monitoring
Whilst the school's focus must always be on educating students about the internet and its use, we also have clear systems and guidelines in place to regulate students' use in school and monitor potentially concerning activity both in school and at home.

We have effective filtering systems to ensure that students use the internet safely in school and are protected from being exposed to extremist, offensive and unpleasant views and material. In addition to this, each device is continually monitored, creating granular alerts of any concerning student online activity on their school device, wherever they are using it. This monitors everything which students type, meaning, for example, that should an inappropriate internet search be unsuccessful and is blocked by a firewall or filtering system, it will still be flagged up as a safeguarding concern.

The school uses Smoothwall to ensure that we have a safe digital learning environment with real-time, content aware and granular control filtering.

Smoothwall
- Keeps users safe by categorising new and existing content in real-time by analysing the content, context and construction of each page.
- Allows our Digital Support Team to build granular controls and web filtering policies based on user group, content category, location IP and time. Each year is separated into their own groups so different policies are applied to different age groups.
- Creates safeguarding reports that notify our CEOP Ambassador and Heads of School of any safeguarding risks, inappropriate content and exploitation.
- Offers appropriate internet access to guest mobile devices securely on our school network across all platforms. Sixth form students operate on bring your own device to ensure that they still only access appropriate information.

The school also operates Google Safe Search as an automated filter of pornography and potentially offensive content. Highfields applies Safe Search to any device connected to the school network; this then applies both in and outside of school.

Any email being sent or received on a school device passes through an Office 365 filter that analyses messages for inappropriate content. If any inappropriate content is found in an email either the Safeguarding team, CEOP Ambassador or Year Team (as appropriate) are notified.

Educating students about online safety
The internet and digital communication are essential elements of 21st Century life for education, business and social interaction. The school has a duty to provide students with high quality internet access as part of their learning experience and to educate them in the appropriate use of digital technologies.

Students will be taught how to:

- Safely and effectively access the internet within clear guidelines for its use
- Use the internet to research; to locate, retrieve and evaluate content
- Be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Publish and present information appropriately to a wider audience
- Report unpleasant internet content e.g. using the CEOP Report Abuse icon and the school's Safeguarding Team safeguardinghighfields@hswv.co.uk

Students are challenged to regularly reflect on their use of the internet and to adopt safe working practices at all times. Online Safety themes are explored as part of the form time programme and in both Digital Life Skills and Citizenship lessons. Online Safety is also given a high profile around school with a range of both traditional and digital display and messages. There are also key points of the year such as Internet Safety Week in which we will use assemblies and other media to further reinforce key messages:

- Think before you post
- Use secure passwords
- Be aware of the risks as well as the opportunities of social networking
- Never give out personal details of any kind which may identify them or their location
- Never place personal photos on any social network space unless privacy settings are in place
- Use nicknames and avatars when using social networking sites
- Digital Wellbeing

Educating parents/carers about online safety
Parents/carers are a key part of supporting students with their safe use of the Internet and we regularly use Welcome and Parents' Evenings to raise awareness of Online Safety. We also have a dedicated Online Safety section on the school website.

We encourage parents/carers to set boundaries for internet usage at home. Bespoke support sessions for parents/carers are available upon request.

Cyberbullying
Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyberbullying, we ensure that students understand how cyber bullying can happen to them and others. We provide students with the information they need to report any concerns they may have that they are a victim of cyber bullying or where they have witnessed an incident.

The school actively discusses cyberbullying with students, explaining why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying.

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the Police if it involves illegal material and will work with external services if it is deemed necessary to do so.

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a good reason to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and Governors/Trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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 students, staff, volunteers, Governors/Trustees and visitors (where relevant) to ensure they comply with the above.

Staff using work devices outside school
Staff members using a work device outside school cannot install any unauthorised software on a device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Work devices must be used solely for work activities.

Staff receive GDPR training and briefings from the Data Protection Officer. Audits are undertaken to ensure that the school is GDPR compliant when handling data.

If staff have any concerns over the security of their device, they must seek advice from the Strategic Infrastructure Manager or the Data Protection Officer.

How the school will respond to issues of misuse
Where a student 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 code of conduct. 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 staff members will receive 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). This training will be delivered via the CEOP Ambassador/Strategic Infrastructure Manager and/or DSL.

The DSL and Deputies will undertake safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors and Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

Monitoring and Review
Updated February 2022