HERSCHEL GRAMMAR SCHOOL

Online Safety Policy 2024

Approved by LGB: March 2024

Date for revision: March 2025

Author: Steve Devereux

Responsibility for Online Safety

Mr Steve Devereux Online Safety Lead (OSL)

Mrs Katrina Rodriguez Designated Safeguarding Lead (DSL)

Young people are growing up in a digital world. As they grow older, they must learn to balance the benefits offered by technology with a critical awareness of the risks and harms they may be exposed to and can expose others to. Herschel Grammar School expects pupils to make a positive contribution online and use technology, the internet and social media as a force for good.

Two of our fundamental values at Herschel are Care and Responsibility. We aim to ensure our pupils are caring, inclusive and respectful in all they do, be it at school, at home, in the broader community and online.

Much of what we do aims to build on the **3 Rs** of:

- respect
- reputation
- responsibility

As well as encouraging the 3 Bs or **3 Ss:**

- Be **S**mart
- Be **S**afe
- Be **S**ure

The key principle of an online safety strategy is understanding the **4 Cs:**

- **C**ontent **being exposed to illegal, inappropriate or harmful content,**
- **C**ontact **being subjected to harmful online interaction with other users**
- **C**onduct **personal online behaviour that increases the likelihood of, or causes, harm**
- **C**ommerce **risks such as online gambling, inappropriate advertising, phishing and or financial scams**

This policy aims to highlight how we aim to achieve the above. The school will be proactive in our work, the online world is a dynamic and 'shifting' place, but at times, the work we must do will be reactive. Therefore, we need to be adaptable when responding to new risks and harms to ensure our pupils stay safe when online both in and outside of school.

We hope to focus our education on underpinning knowledge and behaviours that can help young people navigate the online world safely and confidently regardless of the device, platform or app they use.

We aim to deliver this through a range of approaches such as tutor time, the school bulletin, assemblies, PSHCE/RSE lessons, through more speakers visiting the school and comprehensive pupil and parent engagement and moving forward through our taught curriculums. We are continually updating our website with new and relevant information for parents and young people.

We hope to provide top tips, how-to, advice and support when things don't go to plan and make the most of the online world, such as great apps and sites to support learning. The school purchases and shares with parents Online Safety newsletters and videos covering a whole range of topics delivered by industry expert Alan Mackenzie.

Please visit for more information.

https://www.herschel.slough.sch.uk/School-Information/Online-Safety-1

The school is always looking to develop specific help, information and support pages for our pupils and parents. Each page provides links to sites that offer dedicated support to young people and their families.

Parents, please check out the following page. https://www.herschel.slough.sch.uk/for-parents/online-safety-information

Pupils, please check out the following page. https://www.herschel.slough.sch.uk/For-Students/Online-Safety

The use of the latest technology is actively encouraged at Herschel Grammar School, but with this comes a **responsibility** to protect both pupils and the school from abuse of the system.

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with the latest DfE guidance such as 'Keeping Children Safe in Education' (KCSIE) and other statutory documents; it is designed to sit alongside several school policies, including the Safeguarding Policy, the Behaviour Policy, the Use of ICT policy.

The Designated Safeguarding Lead (DSL) and the Online Safety Lead (OSL) will take responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures when necessary.

This policy aims to:

- Set out expectations for online behaviour, attitudes and activities and use of digital technology
- Create a culture that incorporates the principles of online safety across all elements of school life.
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform
- Facilitate the safe, responsible, and respectful use of technology to support learning, increase attainment, and prepare young people for the opportunities, and risks the online world holds
- Help school staff working with pupils to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
    - establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

This policy applies to all members of the Herschel Grammar School community who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

By the **end of secondary school**, our pupils will know:

- their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- not to provide material to others that they would not want to be shared further and not to share personal material which is sent to them
- what to do and where to get support to report material and suspicious behaviours or to manage issues online
- the impact of viewing harmful content
- that specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours and can damage the way people see themselves in relation to others and negatively affect how they behave toward partners
- that sharing, viewing, and storing indecent images of children (including those created by children) is a criminal offence which carries severe penalties
- how information and data is generated, collected, shared, and used online and the risks of using 'free' applications
- how to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours
- how people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Key responsibilities – All Staff:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up if you have a concern – report it
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- Read Part 1, Annex B of Keeping Children Safe in Education
- Read and follow this policy in conjunction with the school's main Safeguarding policy, Staff Use of ICT Policy, the Staff Code of Conduct and the Behaviour Policy
- Record online-safety incidents in the same way as any safeguarding incident and report, following school procedures, whenever there is a concern with Heads of Learning being a primary contact
- Notify the DSL/OSL if the policy does not reflect practice in school and follow escalation procedures if concerns are not promptly acted upon.
- Identify opportunities to thread online safety through all school activities, both outside the classroom and **within the curriculum**, and make the most of **unexpected learning opportunities** as they arise
- Encourage sensible use, monitor what pupils are doing (when using networked devices in school) and consider the potential dangers and the age-appropriateness of websites and other media when setting work outside of lessons
- Understand **bullying** is also recognised as a type of abuse. It is always distressing for the victim and can have profound consequences and therefore must always be taken seriously and online or cyberbullying is no less serious than physical face-to-face bullying
- Encourage pupils to follow the acceptable use of IT policy (in pupil planners), including any remote learning agreements, remind them about it and enforce school sanctions when not followed
- Notify the DSL/OSL of new trends and issues before they become a problem

- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in communal areas outside the classroom – let the DSL/OSL know if you have a concern
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- Model safe, responsible, and professional behaviours in own use of technology and upholding the reputation of the school and the professional reputation of all staff. – See Use of ICT Policy
- Follow the most current remote learning policy and teacher protocols during any part or full school closure or hybrid teaching
- Understand young people will make mistakes and staff should support them
- Complete regular safeguarding and cybersecurity training.

Bullying happens when an individual or group shows hostility towards another individual, which can be emotional, physical, sexual, or racist. Emotional bullying is by far the most common but sometimes difficult to spot.

Online bullying/Cyberbullying occurs through any online/smart technology such as online chat groups, emails, text messages, online gaming platforms or social networking sites. Online bullying is no less serious than other forms of bullying. Children and young people who use this method of bullying often feel disinhibited from their actions. In addition, it can be particularly distressing for the victim due to the potential 24/7 nature of the abuse.

LGBTQ+ children and children with additional needs can be more at risk and more vulnerable to bullying.

All pupils are made aware of how to report any concerns through the use of our' whisper tool'. All whisper reports are seen by members of the school leadership team.

RESPONSIBILITIES

Online Safety Lead (OSL) Key Responsibilities

- As listed in the 'all staff' section, plus:
- Take an active role in monitoring and investigating online safety violations.
- The OSL will work with the IT Network manager to ensure appropriate filters are in place and to ensure the network remains safe from harm.
- The OSL will be a key member of the Filtering & Monitoring review group. The Filtering & Monitoring groups comprise the DSL, Network Manager and OSL. The groups meet at least once per term to discuss all elements of the approach to Filtering and Monitoring, and to audit the provision again the benchmarks outlined in the latest KCSIE and DfE digital standards.
- The OSL must systematically check the school filtering system and respond to any reports of inappropriate material coming through the filter.
- To record and review any SIMs behaviour logs connected with online safety – recorded centrally as "online safety".
- DSL to update OSL on any issues recorded via CPOMs linked to Online Safety.
- In partnership with DSL to provide training and support to staff, pupils and Parents on Online Safety.
- To develop the strategic plan for IT and Online Learning, maximising the use of IT to facilitate effective teaching, learning and assessment.

- Coordinate and oversee the management and development of IT across the school. In connection with this responsibility, manage the work of both the Network Manager and Online Learning Coordinator
- Develop the use of IT tools to increase the efficiency of administration in the school.
- Develop a consistent approach to online safety in conjunction with the DSL
- Promote online safety messages and engage with parents.

PSHCE Coordinator Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHCE/ RSE curriculum, complementing the existing computing curriculum. Lessons will also cover keeping personal information private, and help young people navigate the virtual world, challenging harmful content, issues surrounding consent, and balancing online and offline worlds.
- Work closely with the DSL/OSL and all other staff to understand the issues, approaches and messaging within PSHCE and RSE.

Head of Computing Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum by following the national curriculum in Computing Technology.
- Work closely with the DSL/OSL/ and Online Learning Coordinator to ensure sufficient coverage of Online Safety at KS3.
- Collaborate with network staff and others responsible for IT use in school to ensure a common and consistent approach, in line with acceptable-use agreements, including remote learning agreements.

Network Manager / IT Support Key responsibilities:

- As listed in the 'all staff' section (where appropriate), plus:
- Keep up to date with the school's online safety policy and technical information to effectively carry out their online safety role and to inform and update others.
- Work closely with the OSL to ensure that school systems and networks reflect school policy in terms of network/server security and the use of specialist software/hardware to protect vital services.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to key systems (especially in terms of access to personal and sensitive records/data and to systems, web filtering settings, and sharing permissions for files on cloud platforms).
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the senior leadership team.
- Maintain up-to-date documentation of the school's security and technical procedures.
- To report online safety issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Monitor the use of school technology (Impero & Senso Cloud) and Microsoft Teams and that any misuse/attempted misuse is identified and reported in line with school policy.

Visitors/contractors Key responsibilities:

- Be made aware of our acceptable use policies.
- Understand safeguarding procedures in place.
- Report any concerns, no matter how small, to the DSL/OSL or the member of staff assigned to their role.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their use of technology

Pupils' Key responsibilities:

- Read, understand and adhere to the pupil acceptable use policy, including the remote learning protocols for pupils.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practices when using digital technologies outside of school and realise that the school's acceptable use policies (including remote learning policies) cover actions outside of school, including on social media.
- Understand that Email, OneDrive and Teams and all activity on the school network (including the VDI) use is monitored.
- Understand the need to keep their passwords strong and secure and are responsible for any actions carried out under their name and must not share passwords or allow others to use their school accounts.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.
- Visit https://www.herschel.slough.sch.uk/For-Students/Online-Safety regularly.
- not sharing other's images or details without explicit permission and not posting negative, threatening or violent comments.
- Use Teams posts and chats to support learning and engagement and not to cause offence or discuss unrelated or irrelevant material.
- Understand that it is illegal to create any online or social media accounts using the school name or logo or badge or masquerade as the school. The school will use any legal route to ensure content is removed.
- Sixth form students who use their own device users cannot attempt to bypass the school filtering, monitoring and security systems through the use of proxy servers, 3rd party software or VPNs and/or by changing the configuration or settings of a computer or portable device. Failure to adhere to this will result in a loss of access to key IT services.

Parents/Carers Key responsibilities:

- Read and promote the school's acceptable use policy that is in the pupil planners and on the school website.
- Consult with the school if they have any concerns about their child's use of technology.
- Promote positive online safety and model safe, responsible and positive behaviours in their use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments.
- Regularly check the parent and pupil Online Safety pages listed above.
- Talk openly with their child about the issues around online safety.

- Regularly checking ParentMail for information on online safety including the Online Safety Newsletter, online safety videos and messaging.
- Parents must ensure their child does not attempt to bypass the school filtering, monitoring and security systems through the use of proxy servers, 3rd party software or VPNs and/or by changing the configuration or settings of a computer or portable device. Failure to adhere to this will result in a loss of access to key IT services.

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHCE, RSE and Computing Technology

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology in school.

We recognise that online safety and broader digital resilience must be thread throughout the curriculum and pastoral systems and always seek opportunities to signpost online safety messages.

Annual reviews of curriculum plans/schemes of work (including for SEND pupils) should be used as an opportunity to focus on the key areas of self-image and identity, online relationships, online reputation, online bullying, managing online information, health, wellbeing and lifestyle, privacy and security, and copyright and ownership.

Handling Concerns

All staff must recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing Technology, PSHCE and RSE).

General concerns must be handled in the same way as any other safeguarding concern. safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture of what might not yet be a problem.

The school's procedures for dealing with online safety are mostly detailed in the following policies (primarily in the first key document):

- Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Staff code of conduct
- Staff use of IT Policy
- Acceptable Use Policy

The school will take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow those responsible to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the OSL on the same day – where urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher unless

the concern is about the Headteacher in which case the complaint is referred to the Chair of Governing Board or the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, the local police and our nominated officer, LGfL, SWGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, CEOP, Prevent Officer, Police, IWF). We will inform, when necessary, parents/carers of online safety incidents involving their child, and the police where staff or pupils engage in or are subject to behaviour which we consider is disturbing or breaks the law or puts them at risk.

SECURITY

Monitoring

The school reserves the right to monitor pupil use of the network, internet, e-mail systems and Microsoft Teams. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached, appropriate action will be taken. For information on staff monitoring, please read the Staff Use of ICT Policy and for pupils read the 'Pupil use of ICT' guidance.

Property

Pupils and staff should treat any property belonging to the school with respect and care and report any faults or breakages to a member of the IT Support staff.

Viruses

Pupils and staff should be aware of the potential damage that computer viruses can cause. The school has banned and restricted the use of portable USB drives. Pupils and staff must not download, install, or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources. Any suspicious email should be reported to IT Support for investigation.

System Security

- The school (summer 2020) upgraded all servers with the latest firmware and updates with extensive use of Microsoft and Sophos protection.
- All computers and servers are updated weekly by Windows Server Update Service, with critical updates being deployed nightly, and security and application updates every week.
- Backup systems are in place to be able to roll back servers. – with devices in a separate building.
- Latest Firewall provision in place, and real-time alerts in place for pupils accessing sever rated material.
- The latest and best industry-standard software to protect from ransomware, malware, exploits and viruses in place across the network.
- At regular intervals, a full cybersecurity/risk management audit will take place.

Leaving workstations

If a user leaves their workstation, they should log out or lock their workstation. Staff can lock their workstations, but only for short periods.

INTERNET

The School recognises the benefits of using the Internet in an educational environment. The Internet facility is provided for school-related activities only. The school monitors the use of the Internet. Age-appropriate filters are in place. However, it is not overly blocked.

The school network system has a real-time monitoring system (Impero), which monitors all onscreen network activity against pre-set policies. Any inappropriate material viewed or written, whether it be sexual, violent, extremist, illegal or inappropriate will be flagged. The network manager, OSL, online learning coordinator and Heads of Learning regularly monitor this.

Viewing, retrieving, or downloading any material by pupils that the school considers inappropriate will result in appropriate action. (Removal or limitation of IT privileges, community service, parental contact, and other appropriate sanctions).

Staff need to ensure that films or other material shown to children are age-appropriate. They must also watch through all clips they intend to show or share before pupils view them either in class or for home learning. This is particularly important for streaming sites (YouTube) that may not have age classifications or content warnings.

Staff must be aware of their responsibilities to the school when using social networking. Our staff Use of ICT policy must be adhered to at all times.

Pupil Messages

- Be careful about publishing any personal information online – like your address, email address or mobile number.
- Think very carefully before posting pictures or videos of yourself or others. Once you've put a picture of yourself online, most people can see it and may be able to download it. It's not just yours anymore.
- Keep your privacy settings as high as possible
- Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do. Remember that not everyone online is who they say they are
- Think carefully about what you say before you post something online especially if you are angry, upset or encouraged by someone else.
- Respecting other people's views, even if you don't agree with someone else's views, doesn't mean you need to be rude or offensive.
- If using social media – make your posts a force for good.
- If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately.
- Use the CEOP website to make a report and use the various reporting tools on the school website.
- The Billboard Test. Before you post something online, think: would you be happy to see it on a billboard where the rest of your school, your parents, your grandparents and neighbours could see it? If not, think twice about sharing online.
- Visit https://www.herschel.slough.sch.uk/For-Students/Online-Safety lots more advice and guidance.
- Be mindful of how often you are online and make sure you are not checking your phone too close to going to sleep and do not check during the night.

Parent Messages

- Parents need to be aware that parental control software is often available via their ISP (broadband provider) so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to

limit the kind of content your children can access through the mobile network.

- Read the online safety newsletters, and try to attend workshops when available.
- Parents need to be aware that parental control software doesn't replace the need for supervision and education when working on the internet.
- Devices for younger children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's online use and discuss various issues about being online.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.
- Parents should discuss the care needed when their children meet online "friends". Only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their children aware of the dangers of meeting someone they have only met online.
- Parents should be aware that they are in control and have every right to check on their children's online activities and mobile usage. However, this must be balanced with a degree of trust and respect for privacy.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities are important.
- Parents should visit https://www.herschel.slough.sch.uk/for-parents/online-safety-information/

Appendix A Mapping for Online Safety

Date	Year 7	Year 8	Year 9	Year 10	Year 11	Year 12	Year 13
	Safer Internet Day Assemblies February 2024all year groups						
Tutor Activities	**Alan Mackenzie Videos are shown during tutor time** Online Bullying Radicalisation Persuasive Design Online Fraud Online Disinhibition Online CSE Mis and Disinformation Employment and Uni Digital Footprint Blackmail / Sextortion						
	Online Safety Video Messages	Online Safety Video Messages	Online Safety Video Messages	Online Safety Video Messages	Online Safety Video Messages	Online Safety Video Messages	Online Safety Video Messages
	Mobile Phone and Internet Safety Resources 1 Resources 2 Resource 3	Bullying and Cyberbullying Resource 1	Healthy relationships online (Childnet) Resources 1	CSE (PC Louise Sloane) Main Hall	Girls and Boys Consent (PC Louise Sloane) Main Hall	Phone/Online Safety Resource 1 Dark Web	Digital Footprint Resource 1
		Sending semi-nude images/ consent (PC Louise Sloane) Main Hall	Bullying vs banter Resources 1	Online Safety Social Media & Self Esteem Sexting and Nudes Resources 1		Sexual Harassment PC Louise Sloane (Main Hall)	Sexual Harassment Resource 1
PSHCE Modules	Device Addiction and Sleep	Bullying Social Media Peer pressure and online	CSE Pornography Sexting / Nudes	Sexting and sending explicit images. Sexual Pressure	online risks and oversharing Speaker	Life skills social media - a force for good.	
	RSE - Consent	sharing and viewing indecent images of children	sharing and viewing indecent images of children	sharing and viewing indecent images of children	sharing and viewing indecent images of children		
				Digital Literacy	Relationships / Pornography		

Appendix B Online Safety Needs – Self Audit for Staff.

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person(s) who has lead responsibility for safeguarding and online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's IT policy for staff?	
Are you familiar with the school's acceptable use agreement for pupils?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling online safety issues?	
Are there any areas of online safety in which you would like training/further training?	
If you are a teacher at Herschel, has your department looked at ways to incorporate Online Safety into the curriculum?	

Appendix C Mobile Phone Use policy for pupils

Year 7 pupils are allowed to bring mobile phones to school but these must be kept in their school bags and must not be used during the school day. Permission must be granted by a member of staff if it is necessary for the mobile phone to be used.

Year 8 and above

Mobile phones should be on "silent" and kept out of sight during lessons/assemblies and registration. On occasions, pupils may have the opportunity to use their mobile phones in the classroom, but only when **express permission has been given by the teacher**.

While on school premises, before and after school and at break times, pupils may use soundless features such as text messaging and vibration alert to receive **important** messages / calls. Any calls made should be of minimal duration and for conveying necessary information rather than for social chat.

We encourage social contact/conversation between pupils, so messaging of friends during break times is discouraged.

Photographs

To safeguard the privacy of all pupils, photographs must not be taken in school, other than in exceptional circumstances.

The school understands that pupils may wish to have photographic memories of special events in school. **Express permission will be given by members of the Senior Leadership Team when photographs may be taken**. Unauthorised taking of images with a camera / mobile phone, still or moving, may result in serious sanctions.

Photographs must never be taken in any situation that may cause embarrassment or discomfort to other pupils, staff or visitors to the school.

If the use of technology humiliates, embarrasses or offends it is unacceptable regardless of whether 'consent' was given.

No photographs must be uploaded to, or shared on, any form of social media.

If requested pupils must show any photographs taken to a member of staff and must delete them if requested.

Security and Safety

The school cannot accept responsibility for any loss, damage or costs incurred due to use. Pupils are expected to hand in mobile phones to PE staff before lessons and are expected to keep phones on their person or in lockers when bags and blazers are left unattended.

For safety reasons phones should not be used when pupils are moving between lessons or around the building.

Pupils should protect their phone numbers by only giving them to close friends and keeping a note of who they have given them to. This can help protect the pupil's number from falling into the wrong hands and guard against the receipt of insulting, threatening or unpleasant voice, text and picture messages.

If a pupil has a problem/ concern during school hours they should talk to a member of staff in the first instance, rather than contacting parents.

Pupils using phones at times that are not permitted will have their phones confiscated until the end of the day. If a phone is confiscated on a number of occasions then the Head of Learning may need to see the phone and check for other usage at non-permitted times. Meetings may be arranged with parents and arrangements made for pupils to bring a phone into school only if it is left with the school office throughout the day.

Appendix D Monitoring and Filtering Provider Checklist (Impero)

Company / Organisation	Impero
Address	Oak House, Mere Way Ruddington Fields Business Park Nottingham NG11 6JS
Contact details	Graham Haythornthwaite VP of Technology Tel: 01509 606540
Monitoring System	Impero Education Pro
Date of assessment	06/07/2018

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

Monitoring Content

Monitoring providers should ensure that they:

Aspect	Rating	Explanation
● Are IWF members		Impero is a member of IWF and has been since 2013. https://www.iwf.org.uk/members/currentmembers
● Work with CTIRU 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Impero has been working with CTIRU since June 2016.

Inappropriate Online Content

Monitoring providers should both confirm, and describe how, their system monitors/manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Illegal	Content that is illegal, for example child abuse images and unlawful terrorist content		Impero Education Pro contains dedicated sets of keyword algorithms that help to identify users who may be engaged in illegal behaviour relating to the searching, distributing or viewing of child abuse images and/or unlawful terrorist content. In relation to child abuse images, the keyword algorithms include specialist terms provided by the Internet Watch Foundation (IWF). These terms are also supplemented with Impero's own research in relation to terminology young people may use in relation to sharing sexual images of themselves online. In relation to unlawful terrorist content, the counter radicalisation and illegal content keyword algorithms include specialist terms provided by a variety of counter extremist and charitable organisations that work at a community level to help reduce race and religious hatred, as well as information from the UK proscribed list of terrorist organisations and the US FTO designated lists. Examples of types of terms used in these algorithms include names of known violent extremist organisations, names of their associated media outlets, and titles of known violent extremist publications/propaganda materials

Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others		Impero Education Pro contains dedicated sets of keyword algorithms that help to identify children who may be engaging in bullying behaviour, either as a bystander or a perpetrator, or help identify a target of such behaviour. The keyword algorithms include phrases relating to bullying behaviours, such as the use of derogatory language based on race, religion, gender, disability, physical appearance and sexuality. Terms relating to name-calling, and threats of violence or put downs are also included. They also include references to people that may be victims of bullying and who are attempting to stop such actions or expressing feelings of being hurt, upset, depression or suicidal. Algorithms are created in conjunction with UK and international charities, such as the Anti-Bullying Alliance, iKeepSafe and Hey U.G.L.Y. Impero has also included input from children and young people gathered through focus group work carried out in schools with pupils.
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet		Impero Education Pro contains dedicated sets of keyword algorithms that help to identify children who may be engaging in risky or inappropriate sexual behaviour online, communicating with strangers, or being coerced into doing something against their wishes. It also helps identify those who may be searching for child sexual abuse content.

Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, sex, disability or gender identity		Impero Education Pro contains dedicated sets of keyword algorithms that help to identify children who may be engaging in discriminatory behaviour or who may hold extreme or intolerant views (in relation to race, religion, gender, disability or a person's sexual orientation). The keyword algorithms include phrases relating to bullying behaviour, common language associated with race and religious hatred, and derogatory language used in relation to the LGBT community. Algorithms are devised in conjunction with input from UK and international charities such as the Anti-Bullying Alliance, Hey U.G.L.Y, HOPE not hate, and iKeepSafe, as well as input from children and young people obtained through focus group work carried out in schools with pupils.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Impero Education Pro contains a dedicated set of keyword algorithms around the area of drug and substance misuse* that helps to identify children that may be engaging in drug use, proactively searching for information on drugs, or talking about drug use in school. The keyword algorithms include common, variant and slang names of known drugs and legal highs, as well as phrases that may indicate the taking of such substances. In addition, each keyword describing a drug name includes an explanation outlining its alternate names, the effects it can have, and its UK and US legal classification.

Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Impero Education Pro contains a dedicated set of keyword algorithms that help to identify children who may be seeking information and/or sharing tips/advice relating to extreme or intolerant views or ideologies, or engaging with others that may hold extreme or intolerant views or ideologies, relating to race, religion, or a person's sexuality. It also detects references to the use of weapons and violence. These keyword algorithms have been developed in conjunction with a variety of specialist organisations ranging from a think tank specialising in countering extremism and terrorism, to charitable organisations that work at a community level to help reduce racial and religious hatred. The keyword algorithms also contain input from specialist safeguarding trainers who deliver Prevent training courses to schools and information from the UK proscribed list of terrorist organisations and the US FTO designated lists. Algorithms also include terms in Arabic.
Pornography	displays sexual acts or explicit images		Impero Education Pro contains a dedicated set of keyword algorithms around the area of adult content. This helps to identify children who may be proactively searching for, or sharing, pornographic images or videos. It also helps to identify children who may be introducing adult content onto the school network. The keyword algorithms include

			common slang terms, acronyms and abbreviations related to adult content and sexual acts, as well as terms that young people may use to deliberately try and evade school filters to find such content.
Self-Harm	promotes or displays deliberate self-harm		Impero Education Pro contains a dedicated set of keyword algorithms around the areas of self-harm, suicide and eating disorders that help to identify children who may be seeking information, sharing tips, or engaging with others on sites of unwelcome persuasion, such as Pro-Ana or Pro self-harm forums. These algorithms have been developed in conjunction with specialists at national charities, such as Harmless, Hey Ugly, Beat (Beating eating disorders), and ANAD (National Association of Anorexia Nervosa & Associated disorders), as well as young people themselves.
Suicide	Suggest the user is considering suicide		Impero Education Pro contains a dedicated set of keyword algorithms around suicide that help to identify children who may be seeking information, sharing suicidal thoughts, or engaging with others on sites of unwelcome persuasion, such as Pro-suicide forums. These algorithms have been developed in conjunction with specialists from leading charities, such as Harmless, Hey U.G.L.Y and iKeepSafe, as well as young people themselves.

Violence	Displays or promotes the use of physical force intended to hurt or kill		Impero Education Pro contains a dedicated set of keyword algorithms around the areas of weapons and violence. Algorithms include explicit references to different types of firearms, knives and other weapons, including makes of such devices, and slang terms for carrying out acts of violence using such weapons or physical force. Impero's anti- bullying algorithms also pick up on threats relating to physical violence. These algorithms have been developed in conjunction with specialists at national charities, such as The Anti-Bullying Alliance, as well as young people themselves.

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Quality and management of content

No monitoring system can be 100% infallible as language and slang terminology is constantly changing and evolving.

To create the lists of key terms used in the software's algorithms, and to try to ensure that these terms are as useful and up-to-date as possible, Impero works closely with specialist expert organisations in the field. Impero also executes its keyword focus group research with students in partnership schools.

Currently, keyword terms are updated at least once a term and include changes made based on customer feedback and/or any new research. We work closely with several partner schools to test our keyword policies in real school environments before release and are constantly improving our policies based on customer feedback.

All keyword terms come with a definition to help explain their significance and why they have been captured. This information helps teachers to understand the context of the term being flagged and assess risk, so they can make good judgement calls on what action to take next - without needing to be experts in all the different aspects of safeguarding issues.
Common misspellings, slang and 'text speak' style terminology is included as standard as part of the algorithms.

If a keyword algorithm is detected, then a screenshot/video recording of the device is triggered along with who, what, where, and when style information so that an incident can be put in context and necessary measures can be taken by staff to open up appropriate dialogues with students and safeguard or manage behaviour accordingly.

Customisation

To help localise their system, schools can add their own bespoke terms to the keyword detection policies, such as student/teacher nicknames, gang names etc. to help identify geographically relevant concerns.

Keyword policy items can be edited or deleted to suit the needs of the school and to help reduce false positives.

Detection settings can be configured to suit different groups of users or devices. For example, a school may want to apply a higher level of detection settings for a particularly vulnerable group of students (such as those who have special needs) and ensure that email alerts are triggered and sent to key-named personnel for any serious captures detected in relation to those students. Likewise, schools may want their 6th formers or staff to have a higher level of access to the internet and lower detection levels for certain keywords.

All detection policies can be scheduled so different policies can apply to different parts of the school day, and can also help with the management of school devices when off-site.

All terms within each policy are customisable in terms of the level of detection and automated related sanctions, e.g. take screen shot, take screen video, log user off, ban the internet for X minutes, send a warning message to the user etc.

Notifications, such as email alerts, can be set to automatically report concerns outside of the system to appropriate members of staff and class teachers can see and manage screenshot captures within their lesson view as they occur.

Managing captures

Impero Education Pro contains inbuilt tools to allow school staff to easily manage, triage and escalate concerns that have been captured.

Captures can be flagged as resolved, under investigation, escalated, or as a false positive, and notes can be added to record any actions taken by staff. All changes to these flags are automatically logged against a user so that a full audit trail of actions taken, and by whom, can be tracked and reviewed.

The log viewer also allows schools to observe patterns of behaviour over time for individual students as well as timeline data, such as what websites a student has visited, what applications they are using, what files they have deleted etc.

It is also possible to export captures to PDF or Excel so that data can be easily shared with other key stakeholders as appropriate and/or added to other relevant school systems, such as a student's behaviour record within the MIS system.

The viewing of captured data logs can be restricted by permissions so that only specified staff members can see an individual's or a group's data and the workload of viewing data can be easily shared and/or partitioned across different members/departments of the school. For example, a school my want to set up viewing permissions by heads of year, pastoral care staff, form tutors, SENCO, DSL, class teacher, or a combination of all of these.

Impero Education Pro also contains classroom control tools and live thumbnail views, providing class teachers the ability to monitor in real time and manage students' use of ICT equipment, helping to break down some of the barriers to using ICT in lessons.

In conjunction with these teaching tools, keyword triggered data captured within a teaching session can also be seen live by the class teacher, so that it can be dealt with there and then, or escalated straight away, in the same way as any other behaviour management or safeguarding issue. The online safety monitoring tools, in combination with classroom teaching tools, means that a whole school approach and a managed approach to online safety can be easily implemented.

Providers should be clear how their system does not overblock access so it does not lead to unreasonable restrictions

The main purpose of the online safety monitoring tools within Impero is to monitor and capture incidents, not to block or restrict content.

If a keyword phrase is detected then a screen shot/screen video of the device is triggered along with who, what, where, when style information so that an incident can be put in context and necessary measures can be taken by staff to open up appropriate dialogues with students. This enables staff to educate, safeguard or manage behaviour.

Although the ability to block against the keyword algorithms or websites when triggered is something that can be set within Impero Education Pro, this is something that is a proactive choice decided by the school themselves against individual terms, or groups of terms, rather than something that is set as standard.

The blocking tools and policies in Impero Education Pro can also be used to give schools the confidence to open up their main filtering system; if students do take advantage of more open access, any untoward sites can be quickly closed down on-the-fly during a lesson using the block functionality within the classroom management tools.

The scheduled policy tools can be used to open up or close access to sites automatically, such as Facebook, for specific time periods, devices or groups of users during the day as required. All terms are customisable in terms of the level of detection and automated related sanctions e.g. log user off, ban the internet for 5 minutes etc. Other automated responses include sending a message to users and sending notifications, such as email alerts to flag concerns outside of the system.

Monitoring System Features

How does the monitoring system meet the following principles:

Principle	Rating	Explanation
Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community-based access		All keyword policies can be set against different user groups (such as year groups) with bespoke detection, filtering and alert settings applied to each of these groups.

• Alert Management – how alerts are managed – if schools manage system alerts or support/management is provided		There are several alert mechanisms which can be configured by the admin of the system and can also be delegated to teachers for configuration where appropriate. There is a live alert within the Thumbnail view, providing a red bar at the top of each thumbnail when a capture has occurred. On custom generated policies, Users can configure a pop-up on each teacher's desktop flagging the nature of the capture, and obfuscating vowels to ensure inappropriate words are not exposed. There is also a pop-up (Toast) option which appears on the desktop of users. Finally, email alerts can be configured by Admin or delegated to staff to send emails to individuals based on a specific group of users/devices, a specific keyword library and/or severity.
• BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (i.e. not owned by the school), how is this deployed and supported and how data is managed. Does it monitor beyond the school hours and location		Impero Education Pro can be installed on an end user's device. A 'Pin Grouping' function is included so that students can login using a pin number; this allows a class teacher to easily group, monitor and manage these devices on an ad-hoc basis.

		For monitoring of devices beyond school hours and outside of the school environment, Impero recommends using its MDM solution, Impero EdLink, in conjunction with Impero Education Pro. This enables both school-owned and student-owned devices to be monitored within and beyond the school's location. Impero EdLink and Impero Education Pro data is managed from within the console and is only accessible by the school.
• Data retention –what data is stored, where is it (physically) stored and for how long		Impero Education Pro is completely configurable. This enables a school to control how long they wish to retain data for and where this data is stored.
• Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers		Impero's products are compatible with Windows, Chrome OS, iOS, Mac OSX and Android.

Flexibility – schools' ability to amend (add or remove) keywords easily		The keyword policies are fully customisable. Terms can be added or removed as required. In addition, individual terms can be edited to change • Severity • Detection settings e.g. trigger only if the term is typed. • Trigger actions e.g. take video capture/lock screen/send message to student/send email alert etc. These edits can be performed on an individual term basis or applied to a batch of selected terms in one go. A school can also set up their own bespoke policies to group related terms together and easily import sets of terms for this purpose.
Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Impero Managed keyword policies are curated by Impero and automatically updated on customer sites, for new keyword policies end users are required to enable the new policies rather than them being enabled by default. End users with multiple Impero instances have the ability to centrally apply configurations on a server and group basis from a central admin console.

Monitoring Policy – How are all users made aware that their online access is being monitored? Is any advice or guidance provided to support schools?		Impero Education Pro contains an Acceptable Use Policy (AUP) display tool that allows schools to display an onscreen AUP or notification message to users when they log in to a device. This on-screen display can be set to appear on every login or the first time a user logs in since the message has been created and activated. Different user groups can receive different on-screen messages. In addition, we always encourage schools to make students aware that they are being monitored and work with you to support your deployment of the system in our handbook we provide template text for AUPs and home school agreements, as well as letters and poster templates to help schools communicate the use of monitoring tools to both students and their parents.
Multiple language support – the ability for the system to manage relevant languages?		The Impero Education Pro system is based on Unicode characters which allows us to support any language.

• Prioritisation – How are alerts generated and prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?		Alerts are triggered by keyword algorithms and their detection settings. All captures within the system are given a severity rating, enabling schools to prioritise these easily. In addition, schools can set up email alerts based on different criteria such as groups of users, types of terms, severity of terms, or a combination of these factors. Alerts are also generated within individual teaching sessions as part of the classroom control interface; a teacher can view captured data relating to their lesson as it occurs and manage accordingly, rather than having to wade through logs retrospectively after a teaching session. Best practice guidance on prioritising, viewing and managing captures is given in the SLT e-safety handbook that accompanies the software.
• Reporting – how alerts are recorded within the system?		All alerts are recorded in real time. If an alert is triggered then a screen shot (and for severe captures, a screen video) is captured, along with detailed information such as the user ID, the device the user was on, time, date, and the trigger term. Once triggered, this data is then recorded in the log viewer, which is a searchable log of all captures across the

		school. If a teacher is using the teaching tools element of Impero then they can also view any captures triggered within their teaching group from the Computer List/Class View or a librarian can view all data triggered within computers in the library, for example.