Orbitaled

British International School
of Ljubljana
an Orbital Education School

British International School of Ljubljana

Online Safety Policy 2023-24

Orbitaled

British International School of Ljubljana

an Orbital Education School

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Principal – Mel Hitchcocks
- Online Safety Officer - (Katarina Zelezinger, DSL)
- Staff – Peter Gombac (IT Manager) and Rachel Burtrand (Tech Leader and IT Teacher)

- **Schedule for Development / Monitoring / Review**

This Online Safety policy was approved by the Board	
The implementation of this Online Safety policy will be monitored by the:	The Principal Team and the Online Safety Group.
Monitoring will take place at regular intervals:	Once a term.
The Regional Head of Schools/ Group Head of IT and the Board will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually unless there are incidents of concern which would necessitate an immediate report. Reportable incidents would also be raised in the Principal's Monthly Report.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2025
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Regional Head of Schools and the Group Head of IT. Infringement of the law would be referred to the appropriate authority.

The school will monitor the impact of the policy using:

- Monitoring internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents, visitors, community users) who have access to and are users of school digital technology systems and networks, both in and out of the school.

The school will deal with such incidents within this policy through the steps outlined in the school´s Positive Behaviour Policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of any inappropriate online behaviour that takes place out of school. In cases where the inappropriate use of the internet has been identified and the student concerned is refusing to handover their device(s), the school reserves the right to conduct a search of the student´s bag and locker. In this case, any search would be conducted by two members of staff of the same sex as the student. The school does not have the right to search a student.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within BISL:

Regional Head of Schools (RHoS) acting on behalf of the Board of Directors

The Board is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the RHoS receiving regular information about online safety incidents and monitoring reports. The RHoS has taken on the role of *Online Safety Operational Board member*. The role of the *Online Safety Operational Board member will include*:

- Termly meetings with the Online Safety Officer (who is the Designated Safeguarding Lead and a member of the SLT – and will be referred to as the DSL throughout the rest of this policy), and the Principal.

- regular monitoring of online safety through incidents logged on the Principals Monthly Report.

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the DSL.
- The Principal and the DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents).
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the DSL. This is to be included in all SLT minutes from Term 2 2024.

Online Safety Officer – the DSL

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides advice for staff - in conjunction with the Tech Lead and IT Manager.
- where necessary liaises with the municipal authority
- liaises with school technical staff – Tech Lead and IT Manager.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Where necessary meets regularly with RHoS to discuss current issues, review incidents

- reports regularly to Senior Leadership Team via weekly SLT meetings.
- Should be aware of the potential for serious child protection / safeguarding issues to arise from:
- sharing of any personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Consequences of online safety incidents

Any incidents which compromise online safety will be dealt with by the DSL and/or the Principal (in her absence, the Director of Teaching and Learning). Breaches will be dealt with on an individual basis and may follow the Positive Behaviour Policy (Students) or Code of Conduct (Staff).

IT Manager / Technical staff

The IT Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any national /municipal / other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which access is logged.
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *network / internet / Learning Platforms such as Canvas and Tapestry / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the DSL and Principal for investigation / action / sanction

- that monitoring software / systems are implemented and updated as agreed with the UK Tech Team.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices by means of regular training (Educare course), events or workshops
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Principal / DSL for investigation / action / sanction
- all digital communications with students and parents should be on a professional level *and only carried out using official school systems*
- **online safety issues are embedded in all aspects of the curriculum and other activities**
- they ensure that students understand and follow online safety procedures and acceptable use policies
- Staff ensure that students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of any personal data
- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Group

The Online Safety Group is a consultative group that is comprised of the DSL, IT Manager and Tech Lead. The group has responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Principal.

Members of the Online Safety Group (or other relevant group) will assist the DSL with:

- the review / monitoring of the school Online Safety Policy / documents.
- mapping and reviewing the online safety provision – ensuring relevance, breadth and progression
- monitoring network / internet
- consulting stakeholders – including parents and the students about the online safety provision.
- The group will meet termly and report back to the Principal. The first meeting of the group (Term 2 – January 2024) reviewed and finalised this policy.

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- will be expected to know and understand school rules on the use of mobile devices and digital cameras. They should also know and understand school rules on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. *The* school will take every opportunity to help parents understand these issues through *parents' evenings*, *newsletters*, *letters*, *website / Canvas/Tapestry and information about national / local online safety campaigns / literature.* Parents will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Canvas or Tapestry and on-line student records
- their children's personal devices in the school (where this is allowed).

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students can freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be made in writing, ideally via email or face to face, with clear reasons given for the need.

Education – Parents

Many parents have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and

young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform(s) such as Canvas and Tapestry
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training (EduCare- Online Safety for International Schools) as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements. The training will be updated every two years.
- This Online Safety Policy and its updates will be reviewed annually by SLT and the working group and shared with staff.
- The working group will provide advice / guidance / training to individuals as required.

Training – Regional Head of Schools and Board

Board members should take part in online safety training / awareness sessions, with importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in several ways:

- Training provided by the Group Head of IT
- Participation of online training provided by relevant organisation such as EduCare.

- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

- **The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: School technical systems will be managed in ways that ensure that the school meets recommended technical requirements and contractors will be supervised when undertaking work on the school system(s).**
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, network equipment, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (*at KS2 and above*) will be provided with a username and secure password by the IT Manager, who will keep an up to date record of users and their usernames. We recommend that staff and students change their passwords every three months. Any users that leave the school will have their account disabled on the last day of association with the school to prevent it being used by others.
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or another person) must also be available to the Principal or other nominated senior leader and kept in the school´s exam safe. Orbital Education can also access the system by changing the master/admin password.
- The IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the firewall appliance, broadband or filtering provider by actively

employing the **Internet Watch Foundation CAIC** list. Content lists are regularly updated, and internet use is logged and regularly monitored. -

- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / students).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place (Helpdesk) for users to report any actual / potential technical incident / security breach to the relevant person, as below. Both the Principal and DSL can be contacted immediately on a face to face basis.
- Appropriate security measures are in place to protect the server, proxy server, firewalls, routers, wireless systems, laptops, tablets, stations, devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. Please see the information below. These are tested regularly. The school infrastructure and individual workstations are protected by up to date anti-virus software, which is centrally managed by Orbital Education.
- An agreed policy is in place (Acceptable Use) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless it has been approved, is safely encrypted or otherwise secured.

Time and date:	14/12/2023	**Completed by:**	Peter Gombac/Jonathan Vazquez
Device type and location checked: *(note device IDs)*	PA-440, Firewall, Security Profiles and Monitoring policies.	**Type of user account / system checked:**	Administrator account

Orbitaled

British International School of Ljubljana

an Orbital Education School

		Any issues ? ✓ or ✗	Actions *(Who, what, how, by when)*
1	**Have all actions from the last filtering checks been completed?**	✓	Jonathan Vazquez checked URL, Application, Antivirus, Anti-spyware, Vulnerability Protection and Zone protection profiles. This was checked on Paloalto firewall device on 14/12/2023 and applied to outgoing traffic.
2	**Is filtering active?** *Non-LGfL school* – ask your technician/provider how best to do this. *LGfL school* – attempt to visit testhomeprotect.lgfl.net / http://wsblock.co.uk * (they should show a block page, NOT load, showing you filtering is active). While on the block page, click to see more information and double check you are on the correct policy, e.g. student policy for a student login (if your provider does not have this on the block page, ask how you can test this).	✓	Web filtering is applied, and details are shared in the "Ljubljana_URL_Filtering.xlsx" file and in screenshots of firewall configuration
	Is the correct policy assigned? *Non-LGfL school* – ask your technician/provider how best to do this. *LGfL school* – while on the block page (eg via above), click to see more information and double check you are on the correct policy, e.g. student policy for a student login (if your	✓	Peter Gombac checks on the monitor tab how the traffic was filtered and through which policy it was filtered by.

	provider does not have this on the block page, ask how you can test this).		
3	**Are the expected categories blocked?** *Non-LGfL school* – ask your technician/provider how best to do this. Beware, if you visit inappropriate sites for testing you should get approval first, log this action for your own protection and consider carefully which to use (e.g. guinness.com, paddypower.com); do not visit real adult sites for testing. *LGfL school* – we have test pages for multiple categories (eg adult/gaming) that you can safely attempt to visit. See note above regarding visits to real sites. Test pages are available via testhomeprotect.lgfl.net or http://testwebscreen.co.uk *	✓	Peter Gombac tests from a device to access several sites that fall in the blocked categories such as:
4	**Are the relevant illegal sites blocked?** Use the Safer Internet Centre's tool at testfiltering.com (select the school button then 'run filtering test'). This covers the IWF and Home Office terrorist and sexual abuse lists. Your provider will also have filed a submission to the Safer Internet Centre with the lists it blocks. *LGfL schools* – note also that LGfL also blocks the City of London Police PIPCU list for pirated film material	✓	Peter Gombac shares a screenshot when accessing this website from a device that is connected to the network.
5	**Is your YouTube mode as expected?** Which of the two restricted modes can you see – visit youtubemode.lgfl.net to test this. Find out more about YouTube modes at youtube.lgfl.net	✗	HTTP header restrictions are on through paloalto safesearch engine on chrome Mozilla, edge still need to be checked for policies
6	**Is Safe Search on and ENFORCED for all search engines you use?** It is vital that this cannot be turned off by users.	✗	Safesearch is enabled in Chrome, however mozilla, edge still needs to be checked for policies

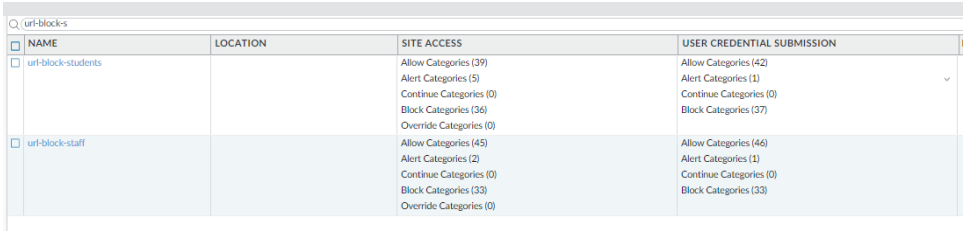
	For Google, visit safesearchcheck.lgfl.net and be sure you cannot toggle it off. (You may wish to block the 'search engine' category for all users and override this only for the one or several which you permit and can guarantee an enforceable safe search for)		URL detailing
7	**Is a website or page which you specifically blocked / unblocked recently or after the last set of checks correct for all users/accounts/devices?** Remember this may be different for different Key Stages or classroom v office staff for example.	✓	Checked on Peters computer and Peter checked on a student's device
8	**Have you asked staff & pupils if they have recently been unable to access educational sites or stumbled across inappropriate sites?** An email reminder to staff whenever you do these checks is wise. Consider what system there is to report instantly (an online form may be better for their responses than email)?	✓	All access is controlled in the way that is detailed in this report. Safesearch is the only pending subject for mozilla and edge web browsers.

** Please note that sites marked http for checking categories etc must be http not https – this is deliberate and is to do with showing individual pages for schools whether they have decryption activated or not. You may be given a browser warning before visiting these pages (which you should otherwise not ignore).*

Ljubljana Firewall Policies

Following below are the details configured on the Firewall for control of the traffic inside the school network:

Global URL Filtering policy for staff and students

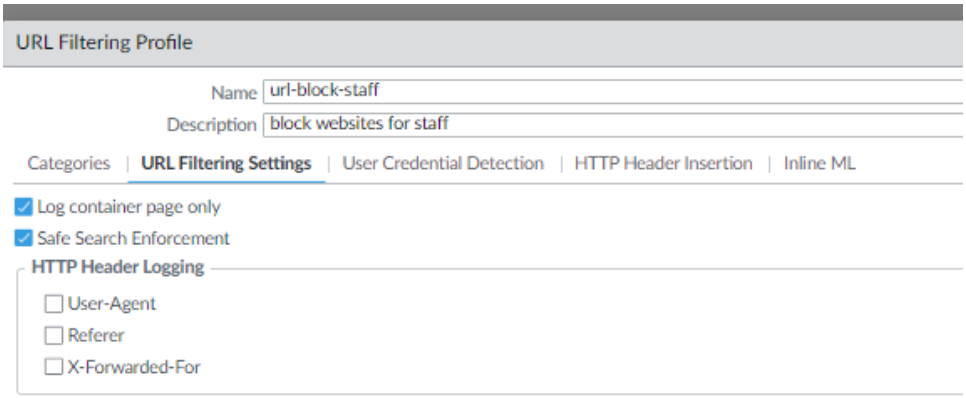


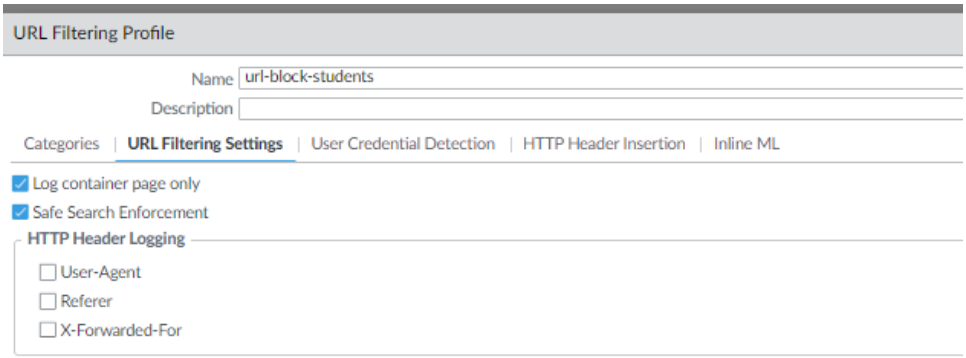
Orbitaled

British International School of Ljubljana

an Orbital Education School

Safe search enabled for staff and students' policies:





URL Filtering by category:

Category	Description	Action
1	Abortion	Deny
2	Abused Drugs	Deny
3	Adult	Deny
4	Alcohol and Tobacco	Deny
5	Auctions	Deny
6	Business and Economy	Allow
7	Command and Control	Deny
8	Computer and Internet Info	Allow
9	Content Delivery Networks	Alert

Orbitaled

British International School of Ljubljana

an Orbital Education School

10	Copyright Infringement	Deny
11	Cryptocurrency	Deny
12	Dating	Deny
13	Dynamic DNS	Deny
14	Educational Institutions	Allow
15	Entertainment and Arts	Allow
16	Extremism	Deny
17	Financial Services	Allow
18	Gambling	Deny
19	Games	Allow*
20	Government	Allow
21	Grayware	Deny
22	Hacking	Deny
23	Health and Medicine	Allow
24	Home and Garden	Allow
25	Hunting and Fishing	Allow

Category	Description	Action
26	Insufficient Content	Deny
27	Internet Communications and Telephony	Allow
28	Internet Portals	Allow
29	Job Search	Allow
30	Legal	Allow
31	Malware	Deny
32	Military	Allow
33	Motor Vehicles	Allow
34	Music	Allow
35	Newly Registered Domain	Deny
36	News	Allow
37	Not-resolved	Deny
38	Nudity	Deny
39	Online Storage and Backup	Allow
40	Parked	Allow
41	Peer-to-Peer	Deny
42	Personal Sites and Blogs	Allow

Orbitaled

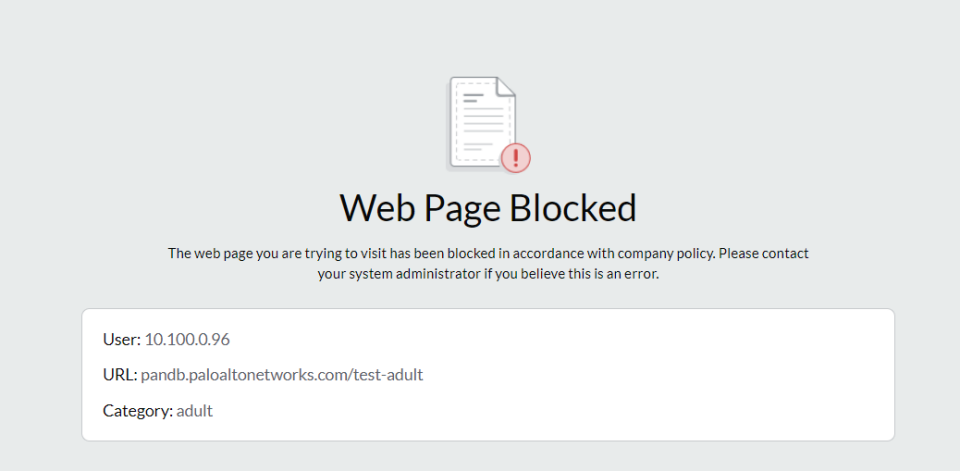
British International School of Ljubljana

an Orbital Education School

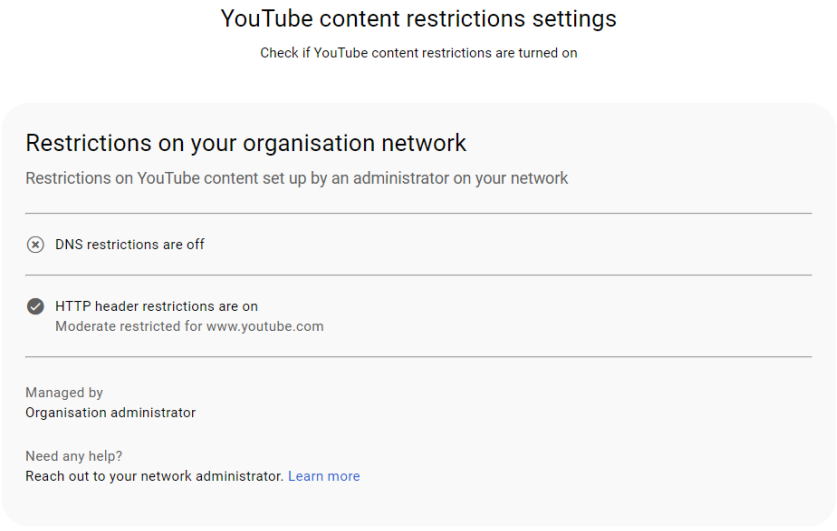
43	Philosophy and Political Advocacy	Allow
44	Phishing	Deny
45	Private IP Addresses	Deny
46	Proxy Avoidance and Anonymizers	Deny
47	Questionable	Deny
48	Real Estate	Allow
49	Recreation and Hobbies	Allow
50	Reference and Research	Allow

Category	Description	Action
51	Religion	Allow
52	Search Engines	Allow
53	Sex Education	Allow*
54	Shareware and Freeware	Deny
55	Shopping	Allow
56	Social Networking	Allow*
57	Society	Allow
58	Sports	Allow
59	Stock Advice and Tools	Allow
60	Streaming Media	Allow*
61	Swimsuits and Intimate Apparel	Deny
62	Training and Tools	Allow
63	Translation	Allow
64	Travel	Allow
65	Unknown	Deny
66	Weapons	Deny
67	Web Advertisements	Deny
68	Web Hosting	Allow
69	Web-based Email	Allow
70	Real-Time-Detection	Deny
71	Ransomware	Deny
72	Encrypted-DNS	Deny
73	Artificial Intelligence	Allow
74	Scanning Activity	Deny

Following is a result of trying to access a blocked website:



Following is the YouTube restriction configuration:



Mobile Technologies (including BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the

capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

The school allows/does not allow the following:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No – student network only*	*Yes – staff network*	*No*
Internet only	*Yes - filtered*	*Yes – filtered*	*Yes - filtered*	*Yes*	*Yes*	*Yes*

Technical support is provided for student owned laptops and iPads. Technical support is not provided for staff or visitors if they are using their own device.

Liability for Personal Devices

Devices owned by students, staff, visitors, are brought into school at their own risk and the school is not liable for the damage or theft of such items. Students in Secondary should store laptops/iPads in their lockers when not in use. Students in Primary should follow the direction of their teachers and store iPads in their classroom when not in use. All personal devices, including mobile phones, should be clearly labelled with the student's name.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

users about these risks and will implement policies to reduce the likelihood of the potential for harm: (select / delete as appropriate)

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents will be obtained before photographs of students are published on the school website / social media / local press.
- Parents are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images **should not** be published / made publicly available on social networking sites, **nor should parents** comment on any activities involving other students in the digital / video images.
- Staff can take digital / video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Ideally, those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes unless necessary (e.g., there is no available school equipment). In the case of a staff member having to use their own device, they must ensure that the images are uploaded to the school IT system as soon as practically possible and before leaving the school site for the day. The images should then be immediately deleted from the staff members personal device.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. The school will not use student photographs on the website or on social media posts without the consent of parents. Consent is given when the student starts at BISL and can be withdrawn at any time.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Following the European Union General Data Protection Regulation (GDPR), Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices, when personal data is stored on any portable computer system, memory stick or any other removable media:
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Orbitaled

British International School of Ljubljana

an Orbital Education School

Communications

Communication Technologies	Staff & other adults			Students				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allow at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	X						X	
Use of mobile phones in lessons		X for lesson demo					X	
Use of mobile phones in social time	X						X	
Taking photos on mobile		X – must be deleted once		X				

phones / cameras		uploaded						
Use of other mobile devices e.g. tablets, gaming devices	X				X			
Use of personal email addresses in school or on school network	X			X				
Use of school email for personal emails	X			X				
Use of messaging apps	X			X				
Use of social media	X			X				
Use of blogs	X						X	

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school / systems (e.g. by remote access).
- Users must immediately report, to the Principal and IT Manager – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while students at KS2 and above will be provided with individual school email addresses for educational use. (Schools may choose to use group or class email addresses for younger age groups e.g. at KS1)
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

- Clear reporting guidance. Any issues relating to child protection/safeguarding should be immediately reported to the DSL. Any issues relating to the inappropriate use of social media by staff should be reported to the Principal.

School staff should ensure that:

- No reference should be made in social media to students, parents or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or Orbital Education
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established, the following guidelines should be followed:

- The account should be approved by the Principal.
- The account should be monitored by at least two members of staff – the member of staff who set up the account and the Principal.
- Any inappropriate use of the account should be reported directly to the DSL (in cases where students are involved) or the Principal.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school. This should be undertaken by Marketing.
- The school should effectively respond to social media comments made by others by Marketing or the Principal only.
- The school's use of social media for professional purposes will be checked regularly by the Principal to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

Orbitaled

British International School of Ljubljana

an Orbital Education School

User Actions		Accept able	Accept able at certain times	Accept able for nominated users	Not accept able	Unaccept able and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm					X
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other					X	

safeguards employed by the school					
Infringing copyright					X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)	X				
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce			X staff only		
File sharing	X				
Use of social media -see above	X				
Use of messaging apps	X staff only				

Use of video broadcasting e.g. YouTube	X				

(The school should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for schools to decide their own responses)

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Orbitaled

British International School
of Ljubljana
an Orbital Education School

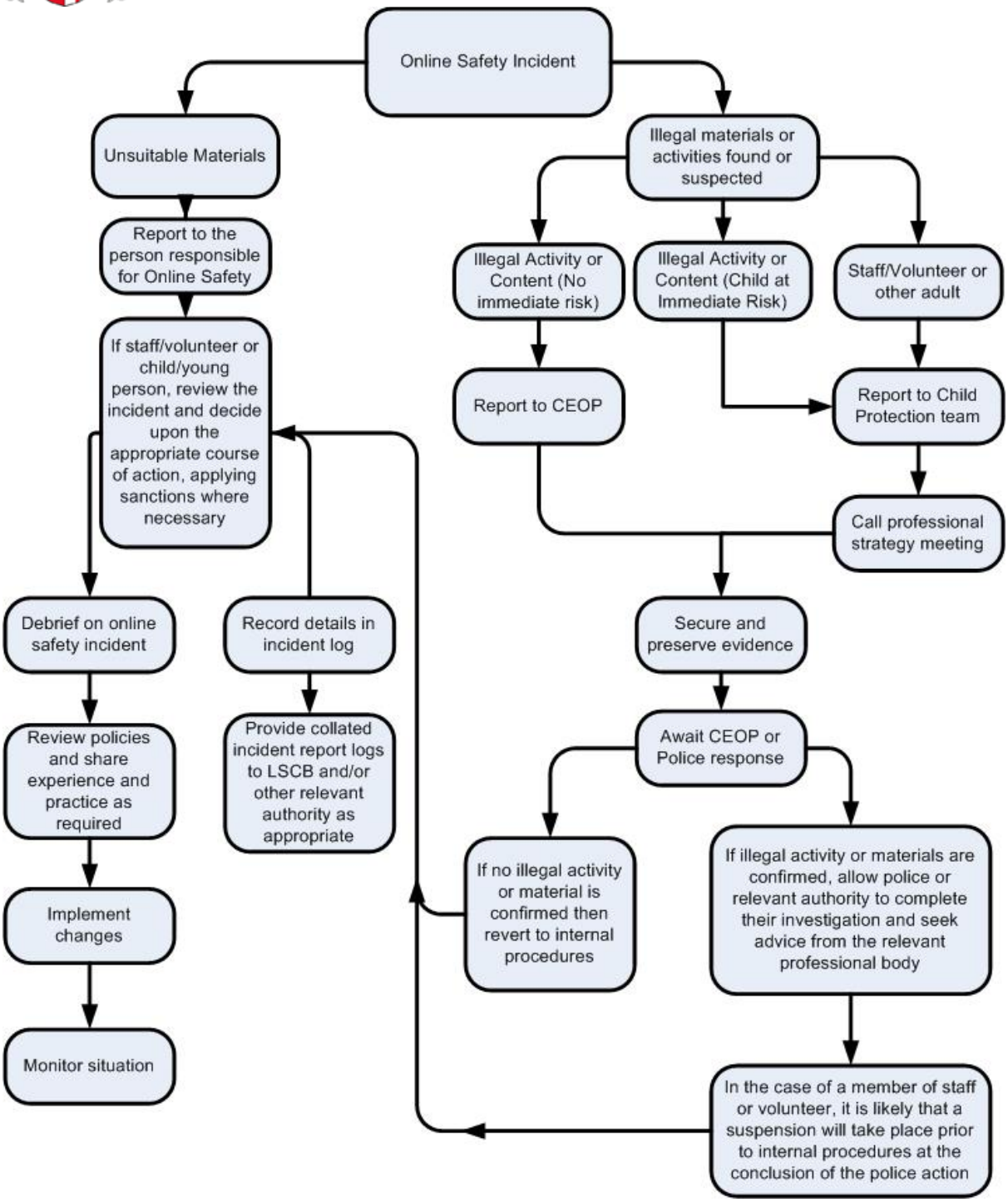
Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the police.

Orbitaled

British International School of Ljubljana

an Orbital Education School



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Try to keep a timeline of investigation events as they are carried out, this will make it easier later if a statement of the chain of events is requested by the police.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the school will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by the Regional Head of Schools/ Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Regional Head of Schools and Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Orbitaled

British International School
of Ljubljana
an Orbital Education School

Students Incidents	Refer to class teacher / tutor	Refer to Head of Department or Principal	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X								
Unauthorised / inappropriate use of mobile phone /	X								

digital camera / another mobile device									
Unauthorised / inappropriate use of social media / messaging apps / personal email	X								
Unauthorised downloading or uploading of files	X	X							
Allowing others to access school network by sharing username and passwords	X	X	X						
Attempting to access or accessing the school network, using another student's account	X	X	X		X	X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X		X

Corrupting or destroying the data of other users	X	X	X		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X		X
Using proxy sites or other means to subvert the school's filtering system	X	X	X	X	X	X	X		X
Accidentally accessing offensive or	X	X	X		X	X	X	X	

pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X		X

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Principal	Refer to RHoS / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X		X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X		X		X	
Unauthorised downloading or uploading of files	X	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X	X		X		X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X	X		
Deliberate actions to breach data protection		X	X	X	X		X	X

or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		X	X				X	X
Actions which could compromise the staff member's professional standing		X	X		X	X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X		X		X	X
Using proxy sites or other means to subvert		X	X		X		X	X

the school's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X		X		X	X
Breaching copyright or licensing regulations		X	X		X	X		X
Continued infringements of the above, following previous warnings or sanctions		X	X	X	X		X	X

Review and Evaluation

This policy is to be review annually, though any deficiencies or weaknesses in arrangements will be remedied without delay.

This policy will be reviewed by the Principal and the Online Safety Group.
Drafted: July 2018
Reviewed: January 2024 by the Online Safety Group and Principal.
Next review: January 2025.