مدرستنا الثانوية الانجليزية – الفجيرة

OUR OWN ENGLISH HIGH SCHOOL - FUJAIRAH

ONLINE SAFETY POLICY

Online Safety Policy

Implemented Date	April 2020
Review Date	February 2021
Next Review Date	September 2021

1. Scope

1 The School is committed to promoting and safeguarding the welfare of all students and an effective online safety is of paramount importance.

2 To apply the principle and culture of reinforcement, encouragement and permanent care to the educational setup, stakeholders and the wider community to reduce behavioural offences inside and outside the walls of the school with the best possible educational means through online safety and promoting values of digital citizenship.

3 Offences and behaviours in the virtual school will be in line with that defines the rules, standards and procedures to be invoked or deal with the students' behaviour in way that it ensures compliance with the school values and systems in line with the ministry online behaviour guidelines for the changing and emerging conditions.

OUR OWN ENGLISH HIGH SCHOOL

1.2 The aims of the School's online safety strategy are threefold:

1.2.1 To protect the whole School community from illegal, inappropriate and harmful content or contact.

1.2.2 To educate the whole School community about their access to and use of technology; and

1.2.3 To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

1.3 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as Technology).

1.4 This policy applies to all members of the School community, including staff, students, parents and visitors, who have access to the School's Technology whether on or off, School premises, or otherwise use Technology in a way which affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.

1.5 The following policies, procedures and resource materials are also relevant to the School's online safety practices:

1.5.1 Acceptable Use Policy for Students
1.5.2 E-learning Cyber Safety policy
1.5.3 Digital well-being policy
1.5.4 MOE Student behaviour Management – Distance Learning
1.5.5 Staff Code of Conduct
1.5.6 Computing Policy
1.5.7 BYOD policy
1.5.8 Acceptable Use Policy for staff

1.5.9 Data Protection Policy
1.5.10 Asset Management Policy
1.5.11 ICT Firewall Policy
1.5.12 Mobile Technologies Policy
1.5.13 Password policy

1.6 This is a whole School policy and applies to Our Own English High School, Fujairah.

2 Roles and responsibilities

2.1 <u>The Governing Body</u>

2.1.1 The Governing Body has overall responsibility for ensuring safeguarding arrangements within the School, including the School's approach to online safety and the use of technology and provide access to appropriate resource required by the IT team and the Principal in safeguarding the online safety of students within the School.

2.1.2 The Governing Body is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of students. The adoption of this policy is part of the Governing Body's response to this duty.

2.1.3 The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in paragraph 1.2 above.

2.2 <u>Principal – Online Safety Leader</u>

2.2.1 The Principal has overall executive responsibility for the safety and welfare of members of the School community.

2.2.2 Act and further develop the role of Online Safety Leader.

2.2.3 In addition to leading the online safety group, she should be ensuring that there is effective online safety training and awareness raising.

2.2.4 Delegate and monitor the duties of Designate Safeguarding Lead in terms of reporting incidents, interventions, training to help the aim and objective are achieved, online safety strategies permeating to all levels.

2.2.5 A developing part of their role should be effective delegation of responsibility to others, ensuring that a wide range of relevant staff owns such responsibilities.

2.2.6 The other referred policies are integrated with online safety and child protection, monitor the awareness of online safety reaches all the stakeholders and wider community.

2.2.7 Curriculum planning and delivery gives scope for cross-curricular links to online safety, cyberbullying, child protection and promote digital citizenship.

2.2.8 Other duties:

- Coordinate with the Board of Governors for the safeguarding arrangements with the school.
- Ensure that the appropriate resources are available in safeguarding the online safety of students within the school.
- Designate a senior member of staff to act on her behalf should she be away from the campus.
- The OSL shall identify training needs and conduct adequate training for all members.
- Review the Esafe policies regularly and bring any matters to the attention of the BOG.
- Advise the governing body on all e-safety matters.
- Liaise with the local authority, IT technical support and other government agencies as required.
- Ensure any technical e-safety measures in the school (e.g. Internet filtering software), are fit for purpose through liaison with the local authority and/or IT Technical Support.

2.3 Senior Leadership Team – Designated Safeguarding Lead

2.3.1 The Designated Safeguarding Leads are senior members of staff from the Senior Leadership Team and the School Counsellor with lead responsibility for safeguarding and child protection. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding & Child Protection Policy.

2.3.2 The Designated Safeguarding Leads will work with the IT Manager in monitoring Technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of students and provide necessary interventions where required.

2.3.3 The Designated Safeguarding Leads will regularly monitor the Technology Incident Log maintained by the IT
Manager and the School Counsellor. The School Counsellor also has a prominent role in safeguarding as mentioned in the cyberbullying, child protection and reporting policy.

2.3.4 The Designated Safeguarding Leads will regularly update other members of the SLT on the operation of the School is safeguarding arrangements, including online safety practices.

2.3.5 Other duties:

- The Designated Safeguarding Lead will regularly update the Principal and other members of the SLT on the operation of the School in safeguarding arrangements, including online safety practices as advised by the Principal.

- The Designated Safeguarding Lead shall ensure the incident logs are maintained by their respective department members.

- The Designated Safeguarding Lead shall ensure that all incidents are appropriately reported and settled. Minutes of all meetings are maintained for future records.

- The Designated Safeguarding Lead shall guide and train teachers on policies, reporting lines, etc. as delegated by the Principal.

- The Designated Safeguarding Leads are senior members of staff from the Senior Leadership Team. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding & Child Protection Policy and instructions, interventions along with the Principal and counsellor where required.

- Responsible for monitoring incidents and handling sensitive issues.

- Keep up to date with the latest risks to staff whilst using technology; familiarize themselves with the latest research and available resources for school and home use.

- Review the esafe policies regularly and bring any matters to the attention of the Principal.

- Update the Principal, governing body on all e-safety matters.

- Engage with staff on e-safety matters at school and/or at home.

- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical e-safety measures in the school (e.g., Internet filtering software), are fit for purpose through liaison with the local authority and/or IT Technical Support.

- Make themselves aware of any reporting function with technical e-safety measures, i.e., internet filtering reporting function; liaise with the Principal and responsible governor to decide on what reports may be appropriate for viewing

2.4 Counsellor:

- The School Counsellor with lead responsibility for safeguarding and child protection along with the Online Safety Leader and Designated Safeguarding Leads.

- All incidents will be reported accordingly to the Principal and Designated Safeguarding Leads.

- Immediately respond when safety incident occurs

- Conducting audit of the online safety incidents, maintain logs and monitoring.

- Assessing the problem

- Determining consequences in accordance with school policies.
- Escalate to the higher authorities.
- Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
- Inform parents, if appropriate, about the incident and how it is being managed
- If appropriate, advise Online Safety Leader for referral to external agencies.

2.5 E-Safety Coordinator (IT Manager)

2.5.1 The IT Manager as E- Safety Coordinator is responsible for ensuring that:

(a) the School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack.

(b) the user may only use the School's Technology if they are properly authenticated and authorised.

(c) the School has an effective filtering policy in place and that it is applied and updated on a regular basis.

(d) the risks of students and staff circumventing the safeguards put in place by the School are minimised;

(e) the use of the School's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and
(f) monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

2.5.3 The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the School to safeguarding issues.

2.5.4 The IT Manager will report regularly to the SLT on the operation of the School's Technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, s/he will escalate those concerns promptly to the appropriate members(s) of the School's Senior Leadership Team (SLT).

2.5.5 The IT Manager is responsible for maintaining the Technology Incident Log and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's Child Protection & Safeguarding Policy and Procedures.

2.6 All staff

2.6.1 The School staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the students.

2.6.2 Staff are expected to adhere, as far as applicable, to each of the policies referenced in paragraph 1.5 above.

2.6.3 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding & Child Protection Policy.

2.6.4 Contribute to this policy and digital citizenship to improve the overall online curriculum of the school.

2.7 Parents

2.7.1 The role of parents in ensuring that students understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:

(a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

(b) talk to their child / children to understand the ways in which they are using the internet, social media and their mobile devices and promote digital citizenship and responsible behaviour;

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support; and

(d) Participate in the Surveys conducted by the school and MOE which helps the school in informing appropriate intervention to be taken.

(e) contribute to the school policies, to be read, understood, acknowledge and provide appropriate feedback.

2.7.2 If parents have any concerns or require any information about online safety, they should contact the DESIGNATED SAFEGUARDING LEAD.

2.8 Students

The role of students to understand how to stay safe when using Technology is crucial. The School expects students to be aware of safe practice when using Technology.

The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching students:

(a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks;

(b) to be critically aware of content they access online and guided to validate accuracy of information;

(c) how to recognise suspicious, bullying, radicalisation and extremist behaviour.

(d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

(e) the consequences of negative online behaviour; and

(f) how to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave inappropriately.

(g) actively participate and contribute to the digital citizenship program.

(h) contribute to this policy via their inputs shared through the Student Digital Safety Leaders and Digital monitors

2.8.1 Student Digital Leaders and Digital Monitors

An essential part of the school’s Online Safety Group is the Student Digital Leaders and the extended online safety group consisting of the Digital Monitors.

a) The Digital Leaders are a part of the School’s Student Council and has representation from all age-groups and phases.
b) They should act as the digital ambassadors or role-models and ideal digital citizens amongst their peers by adopting safe internet practices and digital citizenship.
c) The Digital Leaders should take part in the Online Safety Group meetings and contribute through giving feedback on the Online Safety Policy and all other related policies.
d) They should assist in the Online Safety Education programme assisting the Counsellor and Heads of Sections during the training programmes on Digital Citizenship and Online Safety Education programme.
e) Help the Senior Leaders in evaluating the online safety programme through their feedback.
f) Conduct weekly meetings with the extended Online Safety Group consisting of 70 Digital Monitors representing each Class.
g) Gather feedback and spread awareness on online safety and reporting online safety incidents through the Digital Monitors.
h) Assists the Child protection Officer in terms of safeguarding by reporting incidents and cascading information related to online safety and cyberbullying.
i) Contribute towards the creation of digital content and/or share their expertise in training their peers to create them.
j) Contribute to awareness drives through newsletters, interactive sessions and posters.
k) Support other students in their understanding of online safety, digital safety, digital security, digital identity, digital communication and digital literacy.

2.9 Delegation of Duty:

In the absence of the Principal, the responsibilities will be delegated to the Section Head of CBSE and IGCSE respectively. In the absence of the Section Head, the responsibilities will be delegated to Designated Safeguarding Lead. The E-safety Coordinator and Counsellor will assist the DESIGNATED SAFEGUARDING LEAD and Head of Section.

3 Education and training on Online Safety:

3.1 Students

3.1.1 The safe use of Technology is integral to all School's policies and routines. Students are educated in an age-appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices

3.1.2 Technology is included in the educational programmes followed in the EYFS in the following ways:

(a) children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

(b) children are enabled to explore and play with a wide range of media and materials provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

(c) children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use technology for particular purposes.

3.1.3 The School's Acceptable Use of ICT Policy, BYOD policy, Online behaviour policy for Students sets out the School rules about the use Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology.

Students are reminded of the importance of this policy on a regular basis.

3.2 Staff

3.2.1 The School provides training on the safe use of Technology to staff so that they are aware of how to protect students and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

3.2.2 Induction training for new staff includes guidance on this policy as well as the Code of Conduct, Email & communication Policy and Professional Use of Social Media Guidelines Policy. Ongoing staff development training includes training on Technology safety together with specific safeguarding issues including cyberbullying.

3.2.3 Staff also receive data protection guidance on induction and at regular intervals afterwards.

3.2.4 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

3.3 Parents

3.3.1 We offer the opportunity for parents to attend School based sessions on online safety on a regular basis. Information is available to parents via the school learning portal.

3.3.2 Training and awareness sessions will also be conducted in association with the Parent Advisory Board.

3.3. 3 Parents are encouraged to read the Acceptable Use Policy for Students with their children to ensure that it is fully understood.

4 Access to the School's Technology.

4.1 The School provides laptops, internet and intranet access and an email system to all staff as well as other Technology including but not limited to smart board, OHP, etc. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the ICT.

OUR OWN ENGLISH HIGH SCHOOL

4.2 Students and staff require individual usernames and passwords to access the School's internet and intranet sites and email system which must not be disclosed to any other person.

4.3 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from the IT department in order to use the Wi-Fi.

4.5 Use of mobile electronic devices

4.5.1 The School has appropriate filtering and monitoring systems in place to protect students using the Internet (including email)

4.5.2 The School rules about the use of mobile electronic devices are set out in the Acceptable Use of Technology Policy.

4.5.3 The use of mobile electronic devices by staff is covered in the staff Code of Conduct. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

4.5.4 The School's policies apply to the use of Technology by staff and students whether on or off School premises and appropriate action will be taken where such use affects the welfare of other students or any member of the School community or where the laws of the UAE, its culture or the reputation of the School is put at risk.

5. Offences and Behaviour Categories (As per Ministry of Education-Student Behaviour Management Policy Distance Learning)

5.1 Minor Behaviour Offences

- A delay of (10) minutes or more from the beginning of a distance learning class when broadcasting live without an acceptable excuse

- Wearing clothes that violate public decency and morals while attending the period when broadcasting the distance learning period live
- Private conversations or discourse that are not related to study and hinder the course of the lesson during the live broadcasting of the distance learning period.
- Ridiculing the teacher or a colleague during the distance learning period.
- Eating while attending a distance learning session.
- Adding any unauthorized program, including programs that are shared and free programs.
- Using the microphone feature, camera or chat without prior permission from the teacher.
- Playing games (except with the express permission of the teacher because it is an educational necessity linked to the lesson.)
- Misusing rights and tools available through Microsoft Teams

5.2 Medium Severity Behavioural Offences

- Absence from a single school day (via distance learning) without an acceptable excuse.
- Inciting students not to attend periods, threatening or intimidating them, and not attending periods in distance learning platforms.
- Creating quarrels between students, whether visual or written, by broadcasting via synchronous and asynchronous distance learning platforms.
- Not responding to the rules governing the course of lessons
- Misusing computers during or after the completion of distance education periods.
- Engaging in audio and video communication with the rest of the students for non-educational purposes after the end of the official period time, be it on or off school premises.
- Using e-mail or social media to reveal information of a personal nature.
- Removing the teacher or students from the group that leads to blocking the course of the lesson, teacher’s work and other students' right
- Using profanity, racial slurs, or other language (text, sound, or hint) that may be offensive to any other user.
- Abusing or insulting official visitors during periods during the live broadcast.
- Smoking while attending the distance learning period or possessing any smoking paraphernalia while attending the period.

5.3 Serious Behavioural Offences

- Using the initiative's communication and information technology to insult, curse, threaten with violence, slander, or blackmail in a deliberate and repeated manner via any digital platform
- Participating in unofficial mailing lists and bulletins within the distance education initiative and posting information about teachers and students without permission.
- Posting about the initiative through social media.
- Divulging other students’ personal information, including home addresses and phone numbers
- Searching for information, obtaining specific copies, or modifying files and other data,
- or passwords belonging to other users on the network.
- Entering and using the account of another teacher or student with or without his/her knowledge and/or consent.
- Destroying, modifying, or misusing devices or software in any way.
- Tampering, removing, requesting the removal of, or intentionally causing damage to any device, software or hardware.
- Installing or downloading software or products that might harm the device or the network

- Using any camera (available as part of or as an add-on to certain devices) for personal use, and/or sharing photos or any information about any of the students' parents, employees, or any other person without their explicit consent.
- Using educational content to photograph and recording conversations between students and posting them without prior permission.

5.4 Very Serious Behavioural Offences

- Creating or opening hyperlinks or any associated files unless they are sent from a trusted source.
- Using montage software that can produce unreal and fake content and circulating it on social media.
- Using the network to develop programs that harass users or to penetrate or destroy other people's accounts and devices.
- Establishing networks or network connections to make live communications including audio or video (relay chat) without prior formal permission.
- Publishing, creating, exchanging or promoting malicious or suspicious software.
- Inundating e-mail accounts or applications used for distance education with high electronic data flow, stopping it them working, disabling them or destroying their contents.
- Intentionally capturing or intercepting any communication without authorization through the information network used for distance education.

5.1 PROCEDURES FOR DEALING WITH OFFENCES:

- The following levelled procedures shall be taken, and the deduction of behaviour grades shall be calculated in the event of committing various offences during distance learning, taking into account the detailed instructions and procedures mentioned in the Behaviour Management Policy in public education institutions, and also taking into account the detailed instructions mentioned in the section of procedures for dealing with offences, both according to the degree of the offence that is mentioned in detail in the student Behaviour Management Policy.

- Cases will be presented within the competences of the behaviour management committee, and accordingly, the necessary decisions are taken according to the Behaviour Management Policy in public education institutions (Ministerial Decree No. 851 of 2018).

- In the event that a student with special educational needs or of determination commits a behavioural offence during distance learning, the School Behaviour Management Committee and the school support team shall coordinate with each other and with the special education support centre to study the behaviour of the student to determine the relationship between the offence and the disability, and then apply the same measures mentioned in the 2018 Student Behaviour Management Policy.

- Any breach of these rules (third and fourth-degree offences) may lead to procedures ranging from withdrawing the user's right to log-in or monitoring the use of the service or terminating his/her use of the service or both with retroactive effect. In some cases, it may lead to facing criminal charges, and there will be disciplinary procedures in case of breaching these conditions and rules.

6 Procedures for reporting with incidents of misuse

6.1 Staff, students and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

6.2 Misuse by students

6.2.1 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's E-learning Cyber Safety and Anti bullying policy. Students may report the incident to their teacher or alternatively report anonymously in OSIRS.

6.2.2 Anyone as per the incident reporting policy who has any concern about the misuse of Technology by students should report it as per the incident reporting policy, so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

6.3 Misuse by staff

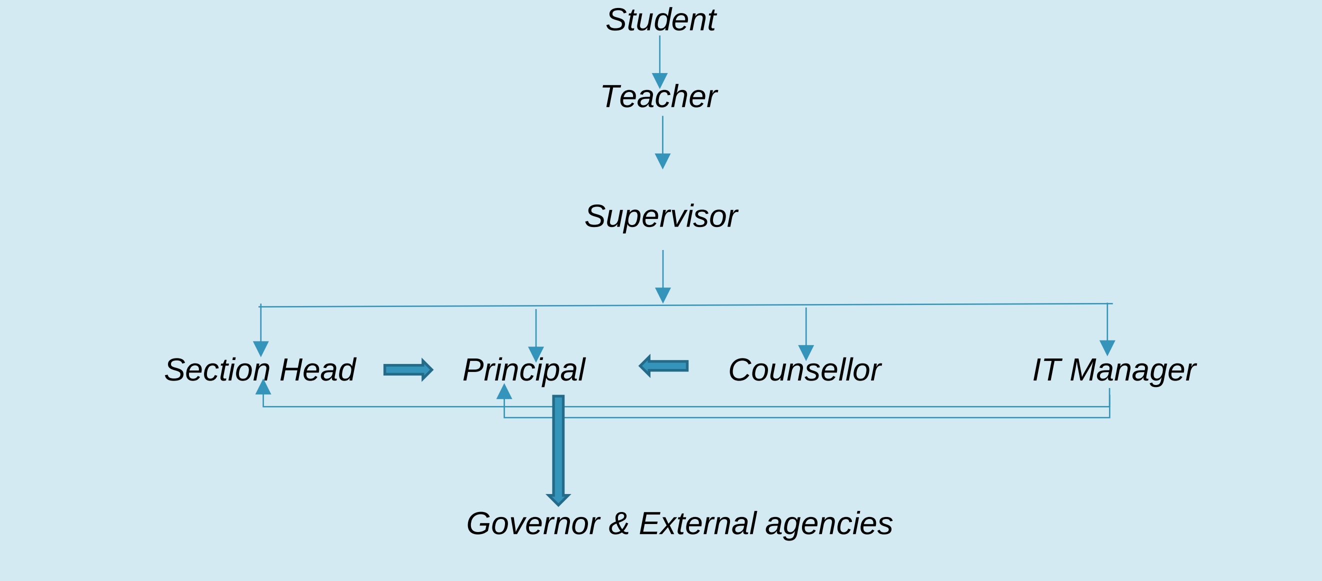
6.3.1 Anyone who has any concern about the online safety or misuse of Technology by staff should report it to their line manager who will escalate it to the Principal so that it can be dealt with in accordance with the staff disciplinary procedures.

6.4 Misuse by any user

6.4.1 Anyone who has a concern about online safety or the misuse of Technology by any other user should report it immediately using the online reporting system (OSIRS)

6.4.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the appropriate government authorities.

Reporting Protocol



7 Monitoring and review

7.1 All serious incidents involving the use of Technology will be logged centrally in the Technology Incident Log by the E-Safety Coordinator.

7.2 The Designated Safeguarding Lead has responsibility for the implementation and review of this policy and will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the School are adequate.

LEAD KINDLY LIGHT