Electronic security policy

1 **Scope of application**

1.1 The School is committed to promoting and safeguarding the well-being of all students, and an effective online safety strategy is fundamental to this.

1.2 The School's online safety strategy has three objectives:

1. Protect the entire school community from illegal, inappropriate, and harmful content or contact;
2. Educate the entire school community about access to and use of technology; and
3. Establish effective mechanisms to identify, intervene, and escalate incidents, when appropriate.

1.3 When considering the scope of the School's online safety strategy, the School will take a broad and intentional approach to consider what falls within the meaning of technology, networks, and devices used to view or exchange information, including communication technology (collectively referred to in this policy as Technology).

1.4 This policy applies to all members of the school community, including staff and volunteers, students, parents, and visitors, who have access to school technology, either on or off school premises, or otherwise use technology in a way that affects the well-being 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:

Anti-Bullying Policy

Staff Code of Conduct

Acceptable Use Policy for Students Protection Policy

1.6 These policies, procedures, and resource materials are available to staff.

1.7 1.7 This is a school-wide policy

2 Duties and responsibilities

2.1 **The Owner / ISP**

2.1.1 The holder has the overall responsibility to safeguard within the School, including the School's approach to online safety and the use of technology within the School.

2.1.2 The owner is obliged 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 owners' response to this duty.

2.1.3 The owner shall conduct an annual review of the School's safeguarding procedures and their implementation, which shall include consideration of the effectiveness of this policy and related policies in meeting the objectives set out in paragraph 1.2 above.

2.2 **Principal and Senior Leadership and Management Team**

2.2.1 The Director has overall executive responsibility for the safety and well-being of members of the school community.

2.2.2 Designated Safeguarding Leaders (DSLs) are senior members of the Senior Leadership and Management Team (SLMT) with primary responsibility for safeguarding and child protection. The DSL's responsibility includes managing protection incidents involving the use of Technology in the same way as other protection matters, in accordance with the School's Safeguarding Policy.

2.2.3 DSLs will work with the Head of ICT and the IT Manager (see below) 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.

2.2.4 DSLs will regularly monitor the Technology Incident Log maintained by the IT Manager.

2.2.5 The DSL will regularly update other members of the SLMT on the operation of the School's safeguarding arrangements, including online safety practices.

2.3 **IT Manager**

2.3.1 The IT Manager, together with his team, is responsible for the effective operation of the School's filtering system, so that students and staff cannot access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

2.3.2 The IT Manager is responsible for ensuring that:

(a) the School's technology infrastructure is secure and, to the extent possible, not open to misuse or malicious attack;
(b) users can only use the School's Technology if they are properly authenticated and authorized;
(c) the School has an effective filtering policy in place that is regularly enforced and updated;
(d) the risks of students and staff circumventing the safeguards put in place by the School are minimized;
(e) the use of the School's Technology is monitored regularly 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 enable the ICT staff to monitor the use of email and the Internet on the School's network and to keep records of such use.

2.3.3 The IT Manager shall provide details, upon request, describing the current technical arrangements and safeguards in place to filter and monitor inappropriate content and alert the School to safeguarding issues.

2.3.4 The IT Manager shall report regularly to the SLMT on the operation of the School's Technology. If the IT Manager has concerns about the functionality, effectiveness, appropriateness, or use of the Technology within the School, he or she shall promptly refer those concerns to the appropriate member(s) of the School's Senior Leadership Team (SLT).

2.3.5 The IT Manager is responsible for maintaining the Technology Incident Log and bringing any safeguarding concerns to the attention of the DSL in accordance with the School's Child Protection and Safeguarding Policy and Procedures.

2.4 All employee

2.4.1 School staff have a responsibility to act as good role models in the use of technology and to share their knowledge of School policies and safe practices with students.

2.4.2 Staff are expected to comply, to the extent applicable, with each of the policies referred to in section 1.5 above.

2.4.3 Staff members are responsible for reporting any concerns about a student's welfare and safety in accordance with this policy and the School's Child Safeguarding and Protection Policy.

2.5 **Parents**

2.5.1 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 practices when using Technology and to:

(a) support the School in implementing this policy and report any concerns in accordance with the School's policies and procedures;
(b) talk to their children to understand the ways in which they are using the Internet, social media, and their mobile devices, and promote responsible behavior; and
(c) encourage your child to talk to someone if they are being bullied or are concerned about their own safety or that of another student or need support.

2.5.2 If parents have any questions or need any information about online safety, they should contact DSL.

Education and training

3.1 **Students**

3.1.1 The safe use of technology is an integral part of the School's ICT curriculum. 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 (see the School Curriculum Policy).

3.1.2 Technology is included in the educational programs followed in the European Year of Fisheries in the following ways:

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

(b) children can explore and play with a wide variety of media and materials and have opportunities and encouragement to share their thoughts, ideas, and feelings through a variety of activities in art, music, movement, dance, drama, design, and technology; and

(c) children are guided to recognize that a variety of technologies are used in places such as homes and schools and are encouraged to select and use technology for specific purposes.

3.1.3 3.1.3 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 technology and how to protect themselves and their peers from potential risks;
(b) to be critically aware of the content they access online and be guided to validate the accuracy of information;
(c) How to recognize suspicious, intimidating, radicalizing, and extremist behavior;
(d) The definition of cyberbullying, its effects on the victim, and how to deal with each of them. Other people's online identities with respect;
(e) the consequences of negative online behavior; and
(f) how to report cyberbullying and/or incidents that make students feel uncomfortable or threatened, and how the School will deal with those who misbehave.

3.1.4 The School's ICT Acceptable Use Policy for Students sets out the School's rules on the use of Technology, including the 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 **Employees**

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

3.2.2 Induction training for new employees includes guidance on this policy, as well as the Staff Code of Conduct, Email and Internet Policy, and Professional Use of Social Media Guidelines Policy. Ongoing staff development training includes training on technology safety, along with specific protection issues, including cyberbullying and radicalization.

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

3.2.4 The frequency, level, and focus of this training will depend on individual roles and needs and will be provided as part of the School's overall approach to safeguarding.

3.3 **Parents**

3.3.1 A 3.3.1 Information is available to parents via the Firefly portal. In addition, we offer parents the opportunity to attend school sessions on online safety annually.

3.3.2 Parents are encouraged to read the Acceptable Use Policy for Students with their son/daughter to ensure that it is fully understood.

3.4 **Usefull Resources**

3.5 There are useful resources on the safe use of technology available through various websites, including:

a) http://www.thinkuknow.co.uk/

b) https://www.disrespectnobody.co.uk/

c) http://www.saferinternet.org.uk/

d) https://www.internetmatters.org/

e) http://educateagainsthate.com/

f) http://www.kidsmart.org.uk/

g) http://www.safetynetkids.org.uk/

h)http://www.safekids.com/

i) http://parentinfo.org/

4 **Access to school technology**

4.1 The School provides Internet and intranet access and an email system for students and staff, as well as other technologies. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the IT Manager and his team.

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. Any student or staff member who has a problem with their username or password must report it to the IT Department immediately.

4.3 No laptop, tablet, or other mobile electronic device may be connected to the School network without the consent of the IT Manager. All devices connected to the school network must have current and up-to-date antivirus software installed and have the latest operating system updates applied. The use of any device connected to the School network will be logged and monitored by the IT Support Department.

4.4 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed regularly, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.

4.1 **4.1** Use of mobile electronic devices

4.1.1 The School has appropriate filtering and monitoring systems in place to protect students who use the Internet (including email, text messaging, and social media sites) when connected to the School network. Mobile devices equipped with a mobile data subscription may, however, provide students with unlimited and unrestricted access to the Internet. As the School cannot provide adequate protection for students, students are not permitted to use their mobile devices to connect to the Internet, including accessing email, text messaging, or social media sites when in the care of the School. In certain circumstances, a student may be given permission to use their own mobile device to connect to the Internet using the School's network. Permission to do so must be requested and given in advance.

4.1.2 The School's rules on the use of mobile electronic devices are set out in the Acceptable Use of Technology Policy for Students.

4.1.3 The use of mobile electronic devices by staff is covered by the Staff Code of Conduct. Unless otherwise agreed in writing, personal mobile devices, including laptops and notebooks, should not be used for school purposes, except in an emergency.

4.1.4 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 when such use affects the welfare of other students or any member of the school community, or when the culture or reputation of the School is put at risk.

5 **5** Procedures for dealing with incidents of misuse

5.1 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 disciplinary and safeguarding policies and procedures.

5.2 **Misuse by students**

5.2.1 Anyone who has concerns about students misusing Technology should report it so that it can be dealt with in accordance with the School's behavior and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

5.2.2 Anyone who has concerns about the welfare and safety of a student should report them immediately in accordance with the School's child protection procedures (see the School's Child Safeguarding and Protection Policy).

5.3 **Misuse by staff**

5.3.1 Anyone who has concerns about the misuse of Technology by employees should report it in accordance with the School's Reporting Policy so that it can be dealt with in accordance with staff disciplinary procedures.

5.3.2 If anyone has a concern relating to safeguarding, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding and Child Protection Policy.

5.4 **Misuse by any user**

5.4.1 Anyone who has a concern about the misuse of Technology by any other user should report it immediately to the Head of ICT or the Principal.

5.4.2 The School reserves the right to withdraw access to the School network from any user at any time and to report suspected illegal activity to the police.

6 **Monitoring and review**

6.1 All serious incidents involving the use of Technology will be recorded centrally in the Technology Incident Log by the IT Manager.

6.2 DSL is responsible for implementing and reviewing this policy and will consider the recording of incidents involving the use of Technology and records of Internet activity (including websites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether the School's existing online safety and protection practices are adequate.

Consideration of the effectiveness of the School's online safety procedures and the education of students on how to stay safe online will be included in the Governors' annual safeguarding review.