مدرستنا الثانوية الإنجليزية ، الشارقة - بنات
Our Own English High School, Sharjah-Girls

GEMS EDUCATION

ONLINE SAFETY POLICY

Implemented : April 2020

Reviewed : May 2026

Next Review : May 2027

Compiled by: SLT &SMT

Approved by: Ms. Asma Gilani, Principal & CEO

Contents

1. Introduction and overview

i. **Scope and definition**
ii. **Roles and responsibilities**
iii. **Communication of the policies**
iv. **Handling complaints**
v. **Review and Monitoring**

2. Education and Curriculum

i. **Online safety/Digital Curriculum**
ii. **Staff training**
iii. **Parent awareness**

3. Online Incident Management

i. **Technological controls**
ii. **Reporting of Online safety incidents**

4. Equipment and Digital Content

i. **Personal mobile phones and devices**
ii. **Digital images and video**
iii. **School website**
iv. **Learning platform**
v. **Social Networking**
vi. **CCTV**

Appendices:

1. *Online Safety Incident Log Form*

1. Introduction and overview

Scope and definition

Scope:

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

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at OOS with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of OOS
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The responsible use of technology is a multi-dimensional, social and behavioural issue. Although the generic term 'E-safety' implies a response to some specific risks (as described below in Understanding the types of E safety risk), we do not regard it as a stand-alone topic. It is embedded within our educational processes and consequently we take a holistic approach to keeping children safe. This policy should therefore be read in conjunction with our other policies, notably:

- Safeguarding
- Anti-Bullying
- Learning for Life (PSHE)
- Wellbeing

Understanding the types of E-safety risk

Risks commonly associated with new media and technology are broad. In most cases the risks are not intrinsically caused by technology, but technology may increase the ease and likelihood of occurrence, and increase the scope of potential harm. Risks include:

1. Predatory behaviours such as grooming, abuse or radicalization,

2. The corruption of young minds through the normalization of disrespectful, or anti-social language and behaviour through exposure to age-inappropriate content[1], especially: violence, pornography, racism, sexism, gambling, advertising, etc.
3. Extensions of 'off-line' peer-behavioural risks, e.g. cyber-bullying, 'trolling',
4. The misplaced perception that aggressive, offensive and inconsiderate on-line language or behaviour is somehow less damaging and more acceptable than their equivalents off-line or face to face.
5. The degradation of educational and maturing processes arising from a child's misplaced judgement of the accuracy, reliability or contextual propriety of online content, Breaking laws, e.g. sexting, copyright infringement, data protection/privacy breaches
6. The lasting damage to self-esteem and to reputation which children may incur (to themselves or to others, thoughtlessly or maliciously) by distributing or publishing confidential, insensitive, offensive or otherwise inappropriate content,
7. Exposure to fraud, hacking or identity-theft through insufficient security of passwords and personal details,
8. The use of new media and technology in distracting or addictive ways.

In order to develop age-appropriate responses to this wide range of risks, we categorise them, along with related learning objectives, as follows (adapted from Tanya Byron's '3 C's of E-safety'):

Risk category	Commercial	Aggressive	Sexual	Values
Content Child is observer/consumer	Understand and develop resilience to advertising, spam, sponsorships and demands for personal information	Develop resilience to violent/hateful content and know how to cope and to deal with it	Avoid/develop resilience to pornographic or unwelcome sexual content	Develop critical evaluation skills to Identify bias, prejudice, misleading and manipulative information and advice
Contact Child is participant	Awareness of tracking, harvesting and the protection of personal information	Develop resilience to being bullied or harassed, and know what actions to take	Understand the implications of interacting with strangers and being groomed	Develop resilience to the risk of compulsive/addictive online behaviour, and to unwelcome persuasions
Conduct Child is instigator/perpetrator	Clear guidance on illegal downloading, copying, plagiarising, hacking, gambling, fraud, identity theft and the consequences	Clear guidance on bullying, harassment or 'trolling' of others and understand the consequences	Clear guidance on creating and uploading inappropriate material and understand the consequences	Clear guidance on the value of personal integrity, respect, data security, confidentiality, and the consequences of publishing inappropriate, false or misleading information or advice

[1] Online games are often cited as one of the principle causes of concern for several of these risks. This may be as much from the highly aggressive and verbally abusive behaviours they elicit as from the be-friending of pseudonymous strangers or from exposure to violent and sexual content. **Extensive exposure to such games may be considered evidence of child neglect**

Roles and responsibilities

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

E-Safety Governor: Ms. Asma Gilani

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

The role of the E-Safety Governor will include:

- To ensure that the school follows all current online Safety advice to keep the students and staff safe.
- To encourage parents and the wider community to become engaged in online safety activities
- Regular meetings with the Online Safety Committee/Officer.
- Regular monitoring of online safety incident logs.
- Reporting to relevant Governors / Board / Committee / meeting.

Designated Safeguarding Lead: Ms. Hemlata Thawani

Designated Safeguarding Lead has the primary responsibility for the implementation and maintenance of this policy.

The role of the Safety Designated Safeguarding lead will include:

- To ensure the safety (including online safety) of members of the school community.
- Responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- To 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 also support to those colleagues who take on important monitoring roles.

Digital Deputy Designated Safeguarding Lead/ Online Safety Officer: Ms. Sheeba Ansar

- Takes day to day responsibility for online safety issues liaising with School safeguarding team and Network Engineer.
- Develops, maintains and quality assures policies and procedures relating to digital technologies and online safeguarding.
- 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 training and resources to staff and students, raising awareness of online safeguarding risks and preventative measures.

- Liaises with school IT Technical Team.
- Receives reports of online safety incidents.
- Ensures that an Online Safety incident log is kept up to date.
- Meets regularly with E-Safety Governor/Child Safeguarding Lead to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meeting / committee of Governors.
- Reports regularly to Senior Leadership Team.
- Is regularly updated in e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying and use of social media
- To oversee the delivery of the Online safety element of the Computing curriculum

Network Officer: Mr. Renson Thomas

The Network Officer is responsible for ensuring that :

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required online safety technical requirements and any SPEA / other relevant body Online Safety Policy / Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Hee keeps up to date with online safety technical information in order to effectively carry out the online safety role and to inform and update others as relevant
- Appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- All data held on students on the school office machines have appropriate access controls in place.
- The use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the / Principal / E- Safety Governor/Designated Safeguarding lead/ Online Safety Officer

Teachers

- To have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- To read, understand and sign the Staff Acceptable Use Policy.
- To report any suspected Online misuse or problem to the Online safety officer for investigation/ action sanction.
- To ensure that all communications with students / parents are on a professional level and only carried out using official school systems.
- To embed online safety issues in all aspects of the curriculum and other school activities.
- To supervise and guide students carefully when engaged in learning activities involving online technology (including, extracurricular and extended school activities).
- In lessons where internet use is pre-planned students should be guided to sites/apps checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. To check with Digital Lead whether the sites/apps are approved by GEMS.
- To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All Staff

- To read, understand and help promote the school's Online Safety policies and guidance.
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy.
- To be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- To report any suspected misuse or problem to the Online Safety Officer.
- To maintain an awareness of current Online Safety issues and guidance e.g. through CPD.
- To model safe, responsible and professional behaviours in their own use of technology.
- To ensure that any digital communications with students should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Students

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- 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.
- Should know whom to contact to report any Online issues.

- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practices when using digital technologies out of school and realize that the school's online Safety Policy covers their actions out of school, if related to their membership of the school.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To provide feedback to review the Online safety policies.

Parents

- To support the school in promoting Online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images.
- To read, understand and promote the school Student Acceptable Use Agreement with their children.
- To access the school Virtual Learning Platform/website/on-line student records in accordance with the relevant school Acceptable Use Agreement.
- To consult with the school if they have any concerns about their children's use of technology
- To provide feedback to review the Online safety policies.

Visitors/External Organisations

- Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school.

Student Ambassadors

- Assist the online safety officer to identify any areas of concern on e- safety in school.
- Organise workshops/talks to help others learn how to be safer online.
- Talk to children across the school about any e-safety concerns that they might have.
- Plan and deliver online safety assemblies/ awareness sessions.
- Keep parents and Governors up to date with current e-safety topics.
- Promote Safer Internet Day and organise whole school activities.

Parent Ambassadors

- Be aware of Health and Safety and child protection issues.
- Recognise issues and concerns regarding Online safety and inform the school in case of any critical incidents.

Roles	Designated person
E-Safety Governor	Ms. Asma Gilani -Principal/CEO
Designated Safeguarding Lead(DSL)	Ms. Hemlata Thawani-Vice Principal
DDDSL/Online Safety Officer	Ms. Sheeba Ansar-Data Supervisor
Network Officer	Mr. Renson Thomas-IT Engineer

ONLINE CONDUCT / BEHAVIOUR COMMITTEE				
Sno	**Name**	**Role**	**Email**	**Designation**
1	Asma Gilani	Conduct Committee Head	asma.g_oos@gemsedu.com	Principal &CEO
2	Hemlata Thawani	Deputy Conduct Committee Head	hemlata.t_oos@gemsedu.com	Vice Principal
Phase wise Online behaviour committee Lead				
3	Priya Ramachandran	KG Lead	priya.r_oos@gemsedu.com	Head of Section- KG
4	Shobhana Sripathi	Primary School Lead	shobhana.s_oos@gemsedu.com	Head of Section - Primary
5	Elizabeth George	Middle School Lead	elizabeth.g_oos@gemsedu.com	Head of Section- Middle School
6	Rachel Pereira	Senior School Lead	rachel.p_oos@gemsedu.com	Head of Section- Senior School
Grade wise Online behaviour committee Lead				
7	Ritu Arora	KG1 Lead	ritu.a_oos@gemsedu.com	KG1 Supervisor
8	Franak Kheshwalla	KG2 Lead	franak.k1_oos@gemsedu.com	KG2 Supervisor
9	Mini Jayapalan	Grade 1 Lead	mini.j_oos@gemsedu.com	Grade 1 Supervisor
10	Samirah Parvez	Grade 2 Lead	samirah.p_oos@gemsedu.com	Grade 2 Supervisor
11	Nandela Sujatha	Grade 3 Lead	nandela.s_oos@gemsedu.com	Grade 3 Supervisor
12	Sharmistha Mazumder	Grade 4 Lead	sharmistha.m_oos@gemsedu.com	Grade 4 Supervisor
13	Sabeena Fakih	Grade 5 Lead	sabeena.f_oos@gemsedu.com	Grade 5 Supervisor
14	Bindu Vijayakumar	Grade 6 Lead	bindu.v_oos@gemsedu.com	Grade 6 Supervisor
15	Vinita Suvarna	Grades 7 and 8 Lead	vinita.s_oos@gemsedu.com	Grade 7&8 Supervisor
16	Reshmi Pillai	Grades 9 and 10 Lead	reshmi.p_oos@gemsedu.com	Grade 9&10 Supervisor
17	Moeen Umrazia Khannum	Grades 11 and 12 Lead	moeen.k_oos@gemsedu.com	Grade 11&12 Supervisor
Online Officers				
Sheeba Ansar		Online Safety Officer	sheeba.a_oos@gemsedu.com	
Renson George		Network Officer	renson.t_oos@gemsedu.com	
School Counsellors & Special Educators				
Student Ambassadors				

Communication of the Policies

Policies will be communicated to staff/students/parents in the following ways:

- Policy to be posted on the Virtual Learning Platform/website / staffroom/ classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with students at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in student/staff personnel files

Handling complaints

- The school will take all reasonable precautions to ensure online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. School **cannot accept** liability for material accessed, or any consequences of Internet access.
- Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by E-Safety Governor/Designated Safety Lead/Online Safety Officer; informing parents;
  - removal of access to school system including School virtual Learning platform/School Student/Curriculum management system -Phoenix;
  - referral to children's services / Police.
- Our Online Safety Officer acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Designated Safeguarding Lead.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school Child safeguarding protection procedures.

Review and Monitoring

The Online safety policy is referenced from within other school policies: Safeguarding Policy, Child Protection policy, Anti-Bullying policy, Behaviour policy.

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The online safety policy has been written by the school online safety officer and approved by Head of School and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders. All amendments to the school e Safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Online Safety/Digital curriculum

This school

- Has a clear, progressive Online safety education programme incorporating Common Sense media digital citizenship curriculum which addresses six core topics of digital citizenship.

Topic Key:	Media Balance & Well-Being	Privacy & Security	Digital Footprint & Identity	Relationships & Communication	Cyberbullying, Digital Drama, & Hate Speech	News & Media Literacy

- These topics covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;

- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies.

The curriculum:

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff training

- Consistent with our Safeguarding policy, all staff receive information and training on Online safety, both at induction, and at regular intervals thereafter (minimum annually),

Parent awareness

- The school runs a guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - Information leaflets; in school newsletters;
    - suggestions for safe Internet use at home;

3. Online Incident Management

Technological controls

In addition to the educational measures to promote Online safety within the curriculum, we maintain specific controls which enable us to establish a secure data and communications environment and to monitor children's digital activity within the boundaries of the school. Foremost amongst these are:

a) Children to whom we provide bespoke[2] access to school ICT resources are asked to agree in writing to a set of rules for the acceptable use of such resources
b) Our password-controlled network maintains individual security, confidentiality and accountability for activity on the network.
c) We use well-established and frequently updated filtering software to prevent access to content deemed to be potentially harmful, and which records attempts to access such potentially harmful content. If staff or children discover unsuitable sites, the URL (web address) must be reported to the Online safety officer. Any member of the school community should report a website which causes them concern to the Online safety officer who will immediately refer this to the Network Officer who will arrange for that site to be blocked.

The scope of the technological controls mentioned above extends across all our network of computers and internet-enabled devices, and across any Wi-Fi access which the school operates.

Whilst these filtering controls can similarly apply to mobile phones which use the school Wi-Fi, we cannot (legally or technically) monitor private phone activity, e.g. texting, or applications or internet content which are accessed via 3G and 4G signals. For this reason, we operate a strict policy on the use of mobile phones.

Our staff are authorised to search for[3] and to confiscate any device, and to search the device and (if appropriate) delete[4] content, if they consider that it is being used in an inappropriate way. Inappropriate usage will be dealt with consistent with our policies on discipline, behaviour, sanctions and exclusions.

[2] School network; unsupervised browsing -BYOD
[3] If in doubt, staff should consult Designated safeguarding Lead
[4] Harmful content may be deleted, unless it is deemed necessary to pass it onto the authorities.

Reporting of Online safety incidents

Any Online safety incident[5], which includes the discovery of a specific or heightened risk, must be reported as soon as possible. If it in any way touches on child safeguarding issues, then it must be reported immediately to the DSL, consistent with the GEMS *Safeguarding policy*. Similarly, if it involves cyber-bullying, then the *Anti-bullying policy* must be followed.

If it relates to technological controls (as described above), or to a breach of the *Acceptable Use policy*, then it must be reported to the Network Officer.

Other members of staff and management should be informed as appropriate in the circumstances.

A log of Online safety incidents should be maintained. The reporting of Online safety Incidents should include the following data:

- Name of person reporting the incident
- Date and time of incident
- Date reported
- Names of people involved
- Location and device details
- Details of incident, including evidence where possible
- Clarification of the risk or breach – e.g. does it relate to safeguarding, bullying, inappropriate content, sexting, data protection, copyright infringement…etc.? Use the 3 C's categorisation as described earlier in this policy.
- Initial action taken and current status

Once investigated, a record of the resolution of the incident, and actions taken as a result, are maintained. Such records are readily available for inspection during governance visits.

Refer Appendix 1

[5] This may be understood as something of a serious nature which requires disclosure and remedial action.

4. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's and parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Student mobile phones which are brought into school (with prior permission) must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- The recording, taking and sharing of images, video and audio on any mobile phone should be avoided; except where it has been explicitly agreed otherwise by the Head of School. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head of School is to be able to withdraw or restrict authorisation for use at any time if it is deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a SLT member.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

Digital images and video

In this school:

- We gain parental permission for use of digital photographs or video involving their child as part of the Social media Consent policy;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

School website

The School Management takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

Names, pictures and content

- Permission will be obtained from parents before any student's image is used.
- Permission will be obtained from parents before publishing the work of any student.
- Children will only be shown in photos where they are suitably dressed.
- Personal details of children or staff such as home addresses, telephone numbers, personal e-mail addresses, etc. will not be released via the website.
- Links to external websites will be checked thoroughly before inclusion on the school website. The sites will be checked for the suitability of their content for their intended audience.
- Any text written by students will be reviewed before inclusion to ensure that no personal details are accidentally included that could lead to the identification of the pupil.
- All written work will be reviewed to ensure that it is in no way defamatory.
- Written work will be checked to ensure (as far as possible) that no copyright or intellectual property rights are infringed.
- All written material will be checked for its suitability for its intended audience.

Privacy

- Adults have the right to refuse permission to publish their image on the site.
- Parents have the right to refuse permission for their child's work and/or image to be published on the site.
- Those wishing to exercise this right should express their wishes in writing to the Head of School, clearly stating whether they object to work, images, or both being published, to the site.

Learning platform

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities
- Photographs and videos uploaded to the schools Virtual learning platform will only be accessible by members of the school community;
- In school, students are only able to upload and publish within school approved and closed systems, such as the Learning Platform

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers 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 local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV

- We have CCTVs in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use it for any other purposes.

Appendix 1

Online Safety Incident Log Form

Name of person reporting incident:	
Date and time of incident:	
Date incident reported:	
Names of people involved:	
Location and device details:	
Details of incident, including evidence:	
Clarification of the risk or breach	☐Cyber bullying/harassment ☐Deliberately bypassing security ☐Accessing unsuitable content ☐Data protection ☐Inappropriate use of technology ☐Inappropriate messages on social media ☐Something inappropriate online Other:……
Initial action taken and current status:	
Resolution of incident:	
Signature	
Date	