



| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

| | |
|--|--|
| Title | E SAFETY POLICY |
| Person responsible for policy formulation, implementation, maintenance and evaluation | Founding Head Master |
| Persons consulted | ELT IT Network Manager Computing Department General Welfare Committee |
| Adopted by College on | 16 September 2016 |
| Status | Review of Original Policy |
| Date of future review | Summer 2024 |

REVISION STATUS TABLE

| Revision No | Effective Date | Summary of Revision | Reviewed | Approved/Noted | |
|-------------|----------------|---------------------------|---|----------------|------------|
| | | | By | By | Date |
| v1.0 | 16 Sep 2016 | New Policy | SMT | FGB | 16.09.2016 |
| V1.1 | 01 Sep 2020 | Review of existing policy | SMT Network Manager Bursar Mr G Proctor, Computing | GWC | 25.09.2020 |
| V1.2 | 09 June 2022 | Review of existing policy | ELT Network Manager Computing department | GWC | 09 June 22 |

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |


POLICY DOCUMENT ANNUAL REVIEW

This policy document is subject to a periodic review by Holyport College that is formally documented to ensure its continuing suitability, adequacy and effectiveness. Areas subject to review include, but are not limited to, follow-up action from previous reviews, policy conformity, review of complaints, status of corrective and preventive actions, and improvements for the forthcoming year. Holyport College reserves the right to amend this policy by notice following such review in circumstances in which it considers such change to be necessary or appropriate.

| | |
|--|-------------------------------------|
| BACKGROUND AND RATIONALE..... | 2 |
| DEVELOPMENT / MONITORING / REVIEW OF THIS POLICY..... | 3 |
| SCOPE OF THE POLICY | 3 |
| ROLES AND RESPONSIBILITIES..... | 3 |
| EDUCATION AND TRAINING | 6 |
| TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND | 7 |
| MONITORING..... | 7 |
| CURRICULUM | 8 |
| USE OF DIGITAL AND VIDEO IMAGES - PHOTOGRAPHIC, VIDEO..... | 9 |
| DATA PROTECTION..... | 9 |
| UNSUITABLE / INAPPROPRIATE ACTIVITIES | 9 |
| RESPONDING TO INCIDENTS OF ABUSE..... | 10 |
| Annex 1 Acceptable Use Agreement..... | Error! Bookmark not defined. |

BACKGROUND AND RATIONALE

Safeguarding is taken very seriously at Holyport College and this includes ensuring our students understand how to stay safe and behave online. We teach students the underpinning knowledge and behaviours which will help them to navigate the online world safely and confidently regardless of the device, platform or app. They are taught what positive, respectful and healthy online relationships look like and the effects of their online actions. We address online safety and behaviour in an age appropriate way, with progression in the content to reflect the different and escalating risks students face.

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

DEVELOPMENT / MONITORING / REVIEW OF THIS POLICY

The policy is reviewed periodically. Any changes to the policy (due to legislative changes or in light of any significant new developments in the use of technologies, new threats or e-safety incidents that have taken place) will be clearly identified. This current policy takes into account the following guidance issued by the Department for Education:

- Relationships Education, Relationships and Sex Education and Health Education, September 2021;
- Teaching online safety in school, June 2019.

Should any serious incidents take place, the DSL will be informed and communication made with Children's Social Care or the Designated Officer if appropriate.

SCOPE OF THE POLICY

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour, including cyber-bullying, or other incidents covered by this policy, which may take place out of school, but is linked to membership of the school. This may include, for example, cyber bullying taking place over the summer holidays and beyond or if a pupil has brought the College into disrepute over social media using a personal device, or from their home.

The College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that takes place out of school. Additional information about cyberbullying can also be found in the anti-bullying policy (see Appendix A)

ROLES AND RESPONSIBILITIES


The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governing Board

- Reviewing the effectiveness of the policy within its remit for safeguarding, delegated to the Governors' Welfare Committee.

Head Master

- Ensuring the safety of the members of the school community, though the day to day responsibility may be delegated;

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

- Ensuring that the relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
- Ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- The SLT will also review any e-safety incidents and discuss them, addressing what had been done well and what could have been done better;
- Should a member of staff need any support following an e-safety incident, the SLT provide support to that individual and confidential counselling is offered if needed.

E-Safety Designated Lead


The Founding Head Master is nominated as the designated e-safety lead. He will liaise closely with House Masters, the IT Network Manager and PD Co-ordinator and will advise on the pastoral aspects of e-safety and the education of e-safety within the College curriculum. Informal liaison will take place on a regular basis and as and when required. The designated e-safety lead will:

- Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies and documents;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Provide training and advice for staff;
- Keep up to date with current e-safety issues and attend conferences and training courses where relevant;
- Liaise with the Safeguarding Team with regards to any e-safety issues which may have a child protection implication;
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments;
- Advise the General Welfare Committee of any e-safety breaches at its termly meeting;
- Debrief to staff with regards any incidents and what might have been learnt from them.

IT Network Manager

The IT Network Manager IS responsible for ensuring:

- That the College's ICT infrastructure is secure and is not open to misuse or malicious attack;
- That users may only access the College's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- The College's filtering procedures are applied and updated on a regular basis and that their implementation is not the sole responsibility of any single person;
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- That the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Founding Head Master for investigation / action / sanction ;

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

- That monitoring software / systems are implemented and updated as agreed in College policies.
-

Teaching and Support Staff

The teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- They have read the Code of Conduct for Staff And Volunteers and understand their obligations with regards to safe and legal use of IT facilities within and owned by the College;
- They report any suspected misuse or problem to the DSL or Head Master for investigation / action / sanction;
- Digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other school activities;
- Students understand and follow the school E-safety and Acceptable Use Policy;
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons and co-curricular activities;
- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to 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;
- They celebrate the positive use of ICT and digital media and promote correct usage;
- It is unacceptable for a member of staff to communicate with students via social media unless it is a school sponsored site that the member of staff is using.


Designated Lead for Safeguarding and Child Protection

The DSL should be trained in e-safety issues and be 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;
- Liaise with Children's Social Care and the LADO when appropriate.

Students

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems;

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

- 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 policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying;
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety Policy covers their actions out of school, if related to their membership of the school.

Parents

Parents also need to be aware that if their children are supplied with a 3G/4G mobile device will be able to access the internet independently of the College system and therefore the College blocking and filtering system will not operate. Parents and carers should educate their own children about digital technology and social media alongside the work that the College undertakes.

Parents and carers will be responsible for:

- Ensuring that they are well – educated themselves on all matters of e-safety. Parents are encouraged to educate themselves on e-safety and attend any events the College may from time to time organise;
- Supporting College actions where an e-safety incident has been dealt with, in line with the Acceptable Use Policy.


EDUCATION AND TRAINING

Education – students

Children and young people need the help and support of the school to learn about e-safety and to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- All pupils will sign the Acceptable Use Policy at the start of each academic year;
- A planned e-safety programme is be provided;
- Key e-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 helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |


school. They should also be educated about protecting their own devices (such as password protecting their mobile and tablets);

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING

The College will be responsible for ensuring that the College infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- There are periodic reviews and audits of the safety and security of College ICT systems. These audits and any action points will be shared with the SLT;
- All users will have clearly defined access rights to College ICT systems;
- All users will be provided with a username and password by IT Services who will keep an up to date record of users and their usernames. Users will be required to have a robust password;
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- The school provides enhanced user-level filtering;
- In the event of the IT Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by Head Master or the designated lead for e-safety;
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Network Manager and referred upwards as appropriate;
- School IT technical staff regularly monitor and record the activity of users on the College ICT systems and users are made aware of this in the Acceptable Use Policy. Monitoring takes place periodically and when triggered by filtering software;
- Appropriate security measures and physical blocks are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data;
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the College system;
- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school workstations / portable devices;
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices;
- Personal data cannot be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |


CURRICULUM

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- 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;
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit by continually moving around the classroom and engaging with the pupils throughout the lesson;
- 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 Network Manager can temporarily remove those sites from the filtered list for the period of study;
- 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.

Our approach to E-safety teaching aims to cover the following:

- Online behaviour
- How to identify online risks
- How and when to seek support
- How to navigate the internet and manage information, including copyright and ownership and privacy and security, age restrictions, disinformation, misinformation and hoaxes, fake websites and scam emails, and phishing
- How content is used and shared, including the targeting of online content on social media and search engines, persuasive design and the importance of a good digital footprint or reputation
- How to stay safe online, including online abuse, challenges, content which incites, fake profiles, grooming, live streaming, pornography and unsafe communication, including the sharing of personal data
- Wellbeing, including the impact on confidence (including body confidence), the impact on quality of life, physical and mental health and relationships, online vs offline behaviours, reputational damage and suicide, self-harm and eating disorders
- The College's SENCO and welfare manager will consider what support, if any, any vulnerable students or students with SEND may need about that which is offered in order to help them stay safe and behave appropriately online.

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

USE OF DIGITAL AND VIDEO IMAGES - PHOTOGRAPHIC, VIDEO

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- Staff are allowed to take digital / video images to support educational aims, but must follow College policy concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment, the personal equipment of staff should not be used for such purposes. If a member of staff wants to use their own equipment they need the permission of the DSL;
- 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. If in doubt, the individual should ask the advice of the DSL;
- Students must not take, use, share, publish or distribute images of other pupils without their permission. It must be recognised by the students that these permissions can change depending on the relationship between particular groups of students;
- 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 College's Term and Conditions clarifies what is permissible and parents are required to opt out of the sharing of such images when signing the College contract. Any images which are published should only use the first name of the student (unless permission has been agreed by the pupil and their parent);
- Particular care should be taken in subjects such as Art, where it may be necessary for students to capture images using digital media of semi-naked models as part of their portfolio work. Advice should be sought from the DSL for safeguarding if there are any concerns;
- Student's work can only be published with the permission of the student.


DATA PROTECTION

- See Data, Information and Records Policy

UNSUITABLE / INAPPROPRIATE ACTIVITIES

The College believes that the activities referred to in the following section would be inappropriate in a school context and that all users of the school IT system should not engage in any of the following activities in school or outside school when using school equipment or systems.

- Child sexual abuse images as laid out in law;
- Promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation;
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist material in the UK;
- Pornography;


| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

- Promotion of any kind of discrimination, racial or religious hatred;
- Threatening behaviour, including promotion of physical violence or mental harm;
- 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;
- Using school systems to run a private business;
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school;
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords);
- Creating or propagating computer viruses or other harmful files;
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet;
- On-line gambling should not be used by any of the pupils in school or outside school when using school equipment or systems. It should be remembered that gambling is illegal under the age of 18.

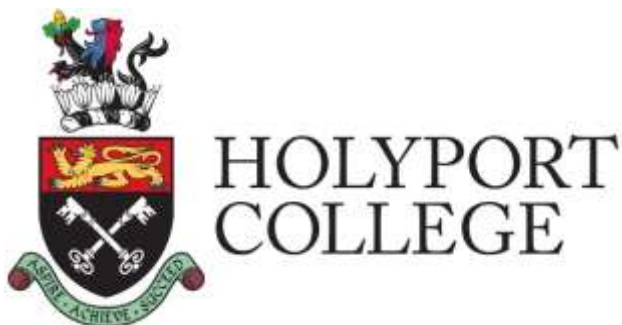
RESPONDING TO INCIDENTS OF ABUSE

When infringements of the policy take place, through careless or irresponsible or, very rarely, through deliberate misuse, such incidents should be reported to the designated lead for Safeguarding. All staff are reminded that there is a clear College Whistleblowing policy, which they should refer to the appropriate person.

The College has a Peer on Peer Abuse policy which covers harmful behaviours students may perpetrate or be a victim of online. The College will report to police and Children's Social Care any incident of online sexual abuse. The College uses the youth service of the Royal Borough of Windsor and Maidenhead to support and educate individuals who are perpetrators or victims of online peer on peer abuse.

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

ANNEXE 1




USE OF MOBILE TELEPHONES AND OTHER DATA AND MEDIA ENABLED DEVICES (SEPTEMBER 2020)

The College permits its students to bring mobile telephones (and other data and media enabled devices) to school provided the student signs up to the following Acceptable Use Agreement and that parents countersign the agreement. If the agreement is not signed by a parent or a student, the student is **not** permitted to bring any electronic devices to the College.


ACCEPTABLE USE AGREEMENT AND LICENCE

The undersigned is entitled to possess and use electronic devices at the College and by signing this agreement undertakes the following:

- I understand that my electronic device is my responsibility and that the College does not accept any responsibility for the loss of or damage to electronic devices or for any costs that arise from the use or misuse of such devices.
- I will protect my electronic devices from misuse by others by locking them with a password or PIN where possible.
- In KS3, I will keep my electronic devices switched off and out of sight between 08.30 and 17.30 and accept that they will be confiscated until the end of the school day if I take them out. If I need to contact my parents in an emergency, I will go to reception and use a College phone.
- In KS4, I will keep my electronic devices switched off and out of sight between 08.30 and 17.30 unless I am using them to listen to music or as a study aid in the prep study area during prep sessions or to listen to music during an art lesson, so long as my teacher has given me permission.
- I accept that my electronic device will be confiscated until the end of the school day if I do not keep to the conditions in this Acceptable Use Agreement.
- I accept that my electronic device cannot be charged up during lessons.

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

- I will only use my electronic device in class under the instruction of the teacher and for educational purposes and will put it away as soon as the activity has ended.
- In Sixth Form, I will model moderate and responsible mobile phone use to younger students.
- I will not take any photos or make video or audio recordings of staff or students without their permission.
- I will not take photos or make video recordings in dorms, toilets or in changing rooms or in any other situation which may cause embarrassment or distress to others.
- I understand that taking/possessing/forwarding photos or video recordings of anyone who is not fully dressed may lead to me being reported to the police for taking/possessing/forwarding an indecent image.
- I will only share photos, video and audio recordings with those I know and only if I have permission of those in the photos or recordings.
- I understand that I have a responsibility to protect my own online reputation and that of the College and of others, and that once something is posted on the internet, it is accessible to lots of people for a very long time. I understand that a poor online reputation can affect my career prospects.
- When on a school trip, I will follow the instructions on the use of electronic devices given by the trip leader and other staff.
- I understand that using my mobile on a trip to a foreign country is expensive and that I will incur roaming costs as smart phones constantly update, even when not in use. I understand that calling or texting friends who are on the same trip can also incur huge costs.
- I understand that cyberbullying can be very upsetting and will only use electronic devices to communicate appropriately with others. I will not use any electronic device to bully, harass or humiliate anyone in any way.
- I will not send threatening or offensive texts or indecent or embarrassing images, or allow others to do so using any electronic device that I own.
- I will not make threatening or offensive calls, or allow others to do so using my phone.
- I understand that I will be punished by the College and/or be reported to the police if I use my electronic devices to cyberbully a member of staff, another student or anyone else, whether or not they are connected to the College.
- I will only download to my electronic devices or access material that is morally decent and appropriate to my age and I will not register for or use services which are restricted for my age group.
- I will not download copyrighted material or share files and understand that the owners of such material may take legal action should I do so.
- I will not attempt to hack into the College's ICT systems and I will not access the personal areas of staff or other students.
- I understand that for examinations I will have to hand in electronic devices for the duration of each particular exam.
- I accept that I may receive a punishment for misuse of electronic devices and that I could lose the privilege of bringing them to the College for a fixed period of time or permanently.

| | | |
|---|----------------------------|------------------|
|  HOLYPORT COLLEGE | E Safety Policy | |
| | Effective Date: 09.06.2022 | Version No: v1.2 |

- I accept that electronic devices may be confiscated if I misuse them and that my parents may be required to collect them from the College.
- I understand that in line with the Education and Inspections Act 2006, I can be punished for using electronic devices outside school in a way which affects the smooth running of the College or the wellbeing of its staff and students.
- I understand that the law permits College staff to confiscate my electronic devices and examine files and data should they have good reason to do so.

DECLARATION:

I understand the terms of this Acceptable Use Agreement and Licence. I understand that failure to comply with its terms will lead to my electronic devices being confiscated and my losing the privilege of using electronic devices at the College for a fixed period of time or permanently. In serious cases, I understand that I may lose my boarding place (if I am a boarder) or be excluded from the College for a fixed term or permanently and I may be subject to Police action and/or prosecution in Court. On conviction, this could lead to me having a criminal record.

Student name:

Date:

Student signature:

Parental Endorsement:

I have read through the above Acceptable Use Agreement with my son or daughter. I agree to support the College in its implementation.

Name:

Signature:

Date: