eSafety and Data Security Policy

Autumn Term 2020

Review Date:	**Autumn Term 2020**
Approved:	**Finance & General Purposes, Autumn 2020**
Ratified:	**Full Governors'**
To Be Reviewed:	**Autumn 2021**
Policy Lead:	**M Giudici**

Holyhead
Teach What Matters

e-Safety and Data Security Policy

CONTENTS

Holyhead
Teach What Matters

e-Safety and Data Security Policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Holyhead school, we understand the responsibility to educate our students on eSafety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (Appendix 1) (for all staff, governors, regular visitors [for regulated activities] and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Related Policies

Our policy relates to e-Safety, staying safe online and data security. Our policy applies to all students, staff (teaching and associate staff), governors and volunteers, temporary and supply staff working in our school. It will be reviewed at least annually by the Governing Body. Other policies that support this policy include:

- Code of Conduct Policies
- Acceptable Use Agreements
- Safeguarding and Child Protection
- School Technical Security Policy (including filtering and passwords)
- Mobile Technologies Policy

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the GDPR, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account. All monitoring, surveillance or investigative activities are conducted by members of the ICT Support team and comply with the GDPR, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to 20 million euros for serious breaches of the General Data Protection Regulations.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows:

- Mark Giudici - IT Manager
- Bernie Maguire - Data Protection Officer

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

Data Protection: key responsibilities for School Principal and Governors

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used
- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response. Previously called a Senior Information Risk Officer (SIRO), there should be a member of the senior leadership team who has the following responsibilities:

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

The Office of Public Sector Information has produced Managing Information Risk, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to:
    - The Waste Electrical and Electronic Equipment Regulations 2006
    - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
    - GDPR
    - Electricity at Work Regulations 1989
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:

    - Date item was disposed of
    - Make, Model and Serial Number
    - How it was disposed of e.g. waste, gift, sale
    - Name of organisation who received the disposed item
- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Email

The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and how to behave responsible online.

Staff and governors should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing email

- The school gives all staff & governors their own email account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- Staff & governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses
- The school requires a standard disclaimer to be attached to all email correspondence. This is done via the Admin console and cannot be changed or deleted.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending emails to external organisations, parents or students are advised to cc. their line manager or designated line manager
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
    - Delete all emails of short-term value
    - Organise emails into folders and carry out frequent house-keeping on all folders and archives
- All students are given an individual school issued account
- All student email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or

arrange to meet anyone without specific permission, virus checking attachments
- Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email
- Staff must inform a member of the ICT Support team if they receive an offensive email
- Students are introduced to email as part of the Computing Programme of Study
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section 'Emailing Personal or Confidential Information'
- Use your own school email account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School email is not to be used for personal advertising.

Receiving emails

- Check your email regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your IT manager first
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of emails is not allowed.

Emailing Personal or Confidential Information

- Where your conclusion is that email must be used to transmit such data:
    - Verify the details, including accurate email address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not copy or forward the email to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an email
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt.

Equal Opportunities

Students with Additional Needs

The school endeavours to create a consistent message with parents/carers for all students and this in turn should aid establishment and future development of the schools' eSafety rules.
However, staff are aware that some students may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and

understanding of eSafety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Principl and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety coordinator in this school is Mark Giudici who has been designated this role as a senior member of staff.

All members of the school community have been made aware of who holds this post. It is the role of the eSafety coordinator to keep abreast of current issues and guidance through organisations such as HCC, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

The Senior Leadership Team and Governors are updated by the eSafety coordinator and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's 'Acceptable Use Agreements' for staff, Governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHCE.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. ESafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in Computing/ICT/ PSCHE lessons. E-Safety, Cyberbullying and the Copyright Act is taught to all Year 7 students as part of the ICT Lesson. In Year 8 the knowledge from Year 7 is re-tested and the following Acts are discussed:- The GDPR, Computer Misuse Act, Health Safety Act and the Copyright Act. Year 9, 10 and 11 students who select OCR ICT or Computer Science will cover the GDPR, Computer Misuse Act, Health & Safety Act and the Copyright Act. In Year 7 PSHCE lessons the students are taught Cyberbullying. As part of this the following topics are discussed: Differences between bullying and Cyberbullying, Why do people bully others, the law surrounding Cyber bullying. In Year 12 the following topics are covered:
    - GDPR
    - Computer Misuse Act -
    - Copyright Legislation
    - Regulation of Investigatory Powers Act -
    - Protection of Freedoms Act 2012
    - The 2002 E-commerce Regulations
    - Equalities Act

- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

<u>eSafety Skills Development for Staff</u>

- Staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of annual e-Safety briefings at the start of each academic year.
- Details of the ongoing staff training programme can be found on the CPD Academic Calendar
- New staff receive information on the school's 'Acceptable Use Policy' as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

<u>Managing the School eSafety Messages</u>

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the students at the start of each school year
- eSafety posters will be prominently displayed
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on.

Incident Reporting, e-Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or e-Safety Coordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Information Asset Owner. See Page 15.

Incident Reporting, e-Safety Incident Log & Infringements

A log is kept of all e-Safety Incidents and Infringements. This is accessible only by members of the ICT Support team.

The following information is recorded on the Incident Log:-

- IncidentID
- Incident
- Student(s)/Staff involved
- Reporting Teacher
- Date Reported
- Time Reported
- Action
- Evidence from IMPERO Logs
- Date and Time Actioned
- Department

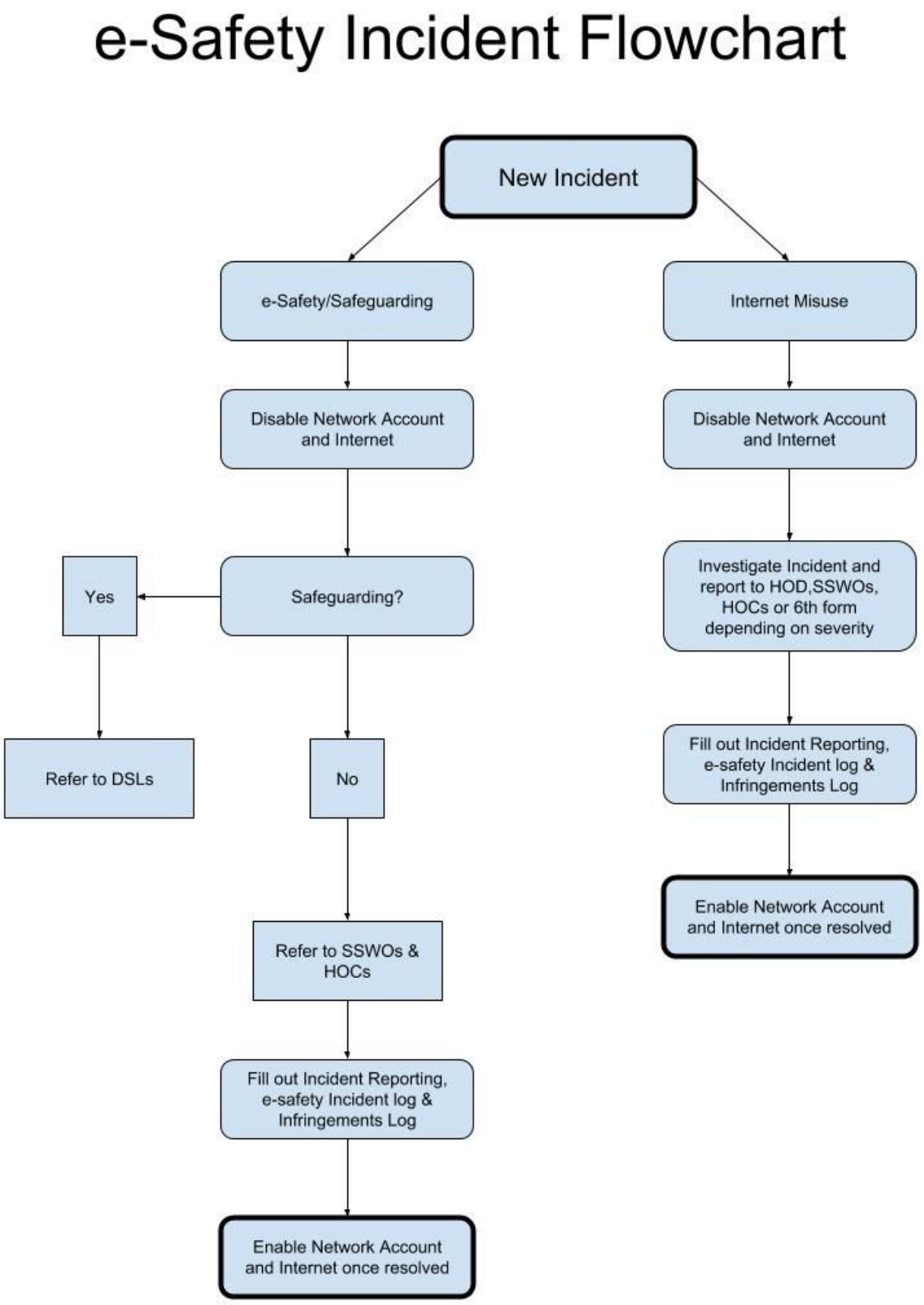
Misuse and Infringements

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Principal. Incidents should be logged and the Flowcharts for Managing an e-Safety Incident should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety coordinator or ICT Support team either by email or Support Request.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Principal. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct during ICT Lessons and Staff CPD

Flowchart for Managing an e-Safety Incident



Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the school network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides students with access to Internet resources through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with students but Google Safe Search is enabled to protect both staff and students.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed.

It is at the Principal's discretion as to what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Holyhead school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; GDPR, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow students access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the ICT Support team, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- The school network will only accept encrypted USB Sticks and all staff and visitors must ensure that their sticks are encrypted before use by a member of the ICT Support team. Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the IT manager's to install or

maintain virus protection on personal systems.
- Students are not allowed to use personal removable media on ANY school device.
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Principal / technician or ICT subject leader.
- If there are any issues related to viruses or anti-virus software, a member of the ICT Support team should be informed.

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to students within school
- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our students are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with students using the school learning platform or other systems approved by the Principal.

Parental Involvement

Holyhead believes that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. The School regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.
- Parents/carers and students are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by (state how)
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement(s) or similar
    - I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.
    - I/we will ensure that my/our online activity would not cause the school, staff,

students or others distress or bring the school community into disrepute.
    - I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube (edit/add services of particular concern here) whilst they are underage (13+ years in most cases).
    - I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information evenings
    - Practical training sessions e.g. current e-Safety issues
    - Posters
    - School website information
    - A Pulse magazine article
    - ParentMail

Passwords and Password Security

Passwords

- Always use your own personal passwords
- Make sure you enter your personal passwords each time you login. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Never tell a child or colleague your password
- If you are aware of a breach of security with your password or account inform a member of the ICT Support staff immediately
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff are removed from the system at the end of their contract. Their Google Drive folder is transferred to their HOD or line manager.
- User ID and passwords for students, who have left the school, are removed from the system immediately and their account deleted after a further 2 months.

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team.

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement (Appendix 1) to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email and Google log-in username. All users are also expected to use a strong personal password and keep it private

- Students are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is as follows:
  - Office Machines - 3 minutes
  - Classroom based teacher machines - 10 minutes
- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)
- At Holyhead, all ICT password policies are the responsibility of the IT Manager and all staff and students are expected to comply with the policies at all times.

Protecting Personal or Sensitive Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal or sensitive information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal or sensitive information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal or sensitive information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal or Sensitive Information Using Removable Media

- Ensure removable media is encrypted by a member of the ICT Support team before you use it.
- Store all removable media securely
- Securely dispose of removable media that may hold personal data as soon as possible after use.
- Only use secure portals for data transfers or encrypt all files containing personal or sensitive data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access

- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Remote Access by 3rd Party companies

- You are responsible for all their activity via their remote access facility for the duration of the support call.
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when the support contractor is working directly with Personal and sensitive data. Do not allow them access unattended.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of students in year 7), students in years 8 - 13 and staff, the school permits the appropriate taking of images by staff and students with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Principal
- Students and staff must have permission from the Principal before any image can be uploaded for publication

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in their personnel file

Publishing Student's Images and Work

On a child's entry to the school in year 7, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school website
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas

- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parent/carers and students over the age of 12 may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Students' names will not be published alongside their image and vice versa. Email and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the ICT Manager, Media Technician Website designer, Deputy Vice Principal and Principal has authority to upload photos to the schools social media platforms.

These include the following:-

- The school's official website
- The school's official twitter account
- The school's official Facebook page
- The school's official YouTube page

<u>Storage of Images</u>

- Images/ films of children are stored on the school's network and secure Google Drive folders
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) unless they are encrypted.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource
- Individual members of staff have the responsibility of deleting the images when they are no longer required, or when the student has left the school

<u>Webcams and Surveillance Cameras</u>

- The school uses surveillance cameras for security and safeguarding. The only people with access to this are The Site Manager and the IT Manager. Notification of camera use is displayed around the school.
- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices

<u>Video Conferencing and Live Zoom Lessons</u>

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school

- All students are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants
- Approval from the Principal is sought prior to all video conferences within school to end-points beyond the school
- All live Zoom lessons are recorded for safeguarding purposes.
- students can only enter a teacher lead live zoom lesson using an invitation linked to their Google Classroom account. They will enter a waiting room and will be let into the lesson by the teacher. Only students who use their full name will be admitted.
- Once admitted their webcams and microphones are automatically muted for safety reasons.
- The host can unmute students as and when required.

Additional points to consider

- Participants in conferences offered by 3rd party organisations may not be DBS checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their unit
    - recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and General Data Protection Regulation (GDPR)

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent
- This technology may be used for educational purposes, as mutually agreed with the Principal. The device user, in this instance, must always ask the prior permission of the bill payer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these

devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for off site visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school
- Never use a hand-held mobile phone whilst driving a vehicle

Telephone Services

- You may make or receive personal telephone calls in designated places, provided:
- They are infrequent, kept as brief as possible and do not cause annoyance to others
- They are not for profit or to premium rate services
- They conform to this and other relevant HCC and school policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that you are available to take any pre-planned incoming telephone calls
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask xxx
- All external telephone calls are recorded. The Telecommunications Regulations 2000 allows companies to record calls to:
- provide evidence of a business transaction
- ensure that a business complies with regulatory procedures
- see quality standards or targets are being met
- in the interests of national security
- for the purpose of preventing or detecting crime
- prevent or detect crime to investigate the unauthorised use of a phone network
- secure the effective operation of the phone network.

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section ‘Storing/Transferring Personal or Sensitive Information Using Removable Media’

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Data must be backed up regularly
- Back up media stored off-site must be secure

Social Media, including Facebook and Twitter

Social media (e.g. Facebook, Twitter, Instagram) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as YouTube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parent/carers and students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation.

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via personal social media accounts.

In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with students are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation

- **Administrator / Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

- **Staff**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via school accounts
  - Adding an appropriate disclaimer to personal accounts when naming the school.

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging

- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

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

- Students
  - Staff are not permitted to follow or engage with current or prior students of the school (with family still attending the school) on any personal social media network account.
  - The school's education programme should enable the students to be safe and responsible users of social media.
  - Students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

- Parents/Carers
  - If parent/carers have access to a school learning platform where posting or commenting is enabled, parent/carers will be informed about acceptable use.
  - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in

person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- The school pro-actively monitors the Internet for public postings about the school and records its on the 'e-safety social media checks' log.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other people's' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, GDPR or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content

- Don’t use social media to air internal grievances

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC at home.
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you log off from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school’s business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are ‘scrubbed’ in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple overwriting the data.

Appendix 1

Student Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people offline that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be Cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involving the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement
.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Student Name:	
Tutor Group:	
Signed:	
Date:	

Appendix 2

Staff and Volunteer Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my own personal devices to record these images. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parent/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are encrypted, protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source

is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Schools Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be secure.
- I understand that eSafety & Data Security Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:

Appendix 3

Use of Digital / Video Images Permission Form

The use of digital/video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally on school controlled social networking sites, these will include Twitter, Facebook and Youtube.

The school will comply with the GDPR and request parent/carer permission before taking images of members of the school. We will also ensure that when images are published, that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the GDPR). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parent/carers comment on any activities involving other students in the digital/video images.

Parent/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Please note: You have the right to withdraw your consent at any time, please email the school on support@holyheadschool.org.uk with your request and it will be processed within 28 working days. We will let you know when this has happened.

Digital/Video Images Permission Form

Parent/Carer Name:	
Student Name:	

Photographs
Please circle either Yes or No for each available item

Do you consent to your photograph being used on the school website?	Yes or No
Do you consent to your photograph being used on displays boards within school?	Yes or No
Do you consent to your photograph being used in the Pulse magazine?	Yes or No
Do you consent to your photograph being used in the school prospectus?	Yes or No
Do you consent to your photograph being displayed via the school's Twitter & Facebook feed	Yes or No
Do you consent for recorded footage of you to be used on the school's	Yes or No

YouTube feed	
Do you consent to your photograph being used by the RSA?	Yes or No
Do you consent to your photograph being used by the RSA Academy?	Yes or No

Videos
Please circle either Yes or No for each available item

Do you consent for recorded footage of you to be used on the school's website?	Yes or No
Do you consent for recorded footage of you to be used on the school's YouTube feed?	Yes or No
Do you consent for recorded footage of you to be displayed via the school's Twitter & Facebook feed?	Yes or No
Do you consent for recorded footage of you to be used by the RSA?	Yes or No
Do you consent for recorded footage of you to be used by the RSA Academy?	Yes or No

3rd Party Companies
Your child may get invited to participate in external events run by 3rd Party companies (for example The BBC, The REP Theatre Company etc)

Please circle either Yes or No for each available item

Do you consent for recorded footage of you to be used by these 3rd party companies?	Yes or No
Do you consent to your photograph being used by these 3rd party companies?	Yes or No

I agree that if I take digital or video images at, or of , school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes or No

Parent Signature

Parent Name	
Parent Signature	
Date	

Appendix 4

Use of Cloud Systems Permission Form

The school uses Google Apps for Education for students and staff. This permission form describes the tools and student responsibilities for using these services.

The following services are available to each student and hosted by Google as part of the school's online presence in Google Apps for Education:

- **Mail** - an individual email account for school use managed by the school
- **Calendar** - an individual calendar providing the ability to organize schedules, daily activities, and assignments
- **Google Drive** - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Using these tools, students collaboratively create, edit and share files for school related projects and communicate via email with other students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent/Carer Name:	
Student Name:	

As the parent / carer of the above student, I agree to my child using the school using Google Apps for Education.	**Yes**	**No**

Signed:	
Date:	

Appendix 5

COVID-19 Live Learning / Video Learning - Parent/Guardian & Student Agreement.

This will need to be accompanied by a students and parent consent form submitted via Arbor.

During the current school closures we are delivering all of our learning remotely. In order to make this process as effective and as engaging as possible we are utilising a variety of new technologies and teaching strategies. Increasingly staff are making use of video technology to record themselves delivering key concepts, modelling how to complete the activity, providing generic feedback or explaining the next steps of the learning.

This is going to be an important element of our teaching and learning strategy and, as such, we need to ensure that all students and parents are aware of, and agree to, the **Remote Learning Behaviour Agreement** outlined below. This will ensure that our staff can be as creative as possible when engaging with our students in their learning.

The agreement below is developed within an overarching aim to provide the very best teaching and learning for our students whilst at the same time protecting our staff. It is essential that all parties are respectful of each other and that the use of video technology does not become an invasion of privacy.

Parental Agreement
I / We agree to support the teaching and learning strategies and increased use of video lessons and live lessons by discussing and reinforcing the expectations identified below. I / We have read the 'Student Agreement' and understand that the agreement is important for the safeguarding of all parties. I understand that breach of this agreement will lead to sanctions and in the event that videos are taken and placed on social media could lead to exclusions, permanent exclusion or police involvement. The school reserves the right to seek legal advice in situations which may be libelous or result in defamation of character.

Student Agreement
I confirm that I have read the 'Learning Behaviour Agreement' and 'General Learning Expectations' below and agree to adhere to it in order to enable teaching staff to make the best use of technology, to provide purposeful and engaging learning during a period of school closure. I understand that breach of this agreement will lead to sanctions and in the event that videos are taken and placed on social media could lead to exclusions, permanent exclusion or police involvement. The school reserves the right to seek legal advice in situations which may be libelous or result in defamation of character.

Learning Behaviour Agreement - where a teacher uses a recorded video / live video or audio message to support learning:

- I agree that I must never use some or all of this material for any purpose other than my own learning.

- I will never place any of a teacher's video or audio file on any on-line platform or social media platform.
- I will not record any part or whole of a live video or pre-recorded lesson.
- I will not edit any part or whole of a live video or pre-recorded lesson.
- I agree that my teacher will always record any live video lesson; I understand that this is an agreement to ensure the safety of all students and teachers.
- If I am involved in a live lesson I agree to ensure that I am aware of others in my own home and that they know I am engaged in a lesson to avoid unnecessary or inappropriate distractions.
- If I am involved in any live video lesson I will ensure that I am wearing sensible and appropriate clothing that would be deemed acceptable on a school non-uniform day.
- I understand that my teacher may be recording or delivering the lesson from their own home and that I should be respectful that this is their private space and is not a subject that should be discussed with them or with others.
- I understand that other students will also be inside their homes, which may also be visible on camera, and that I should be respectful that this is their private space and is not a subject that should be discussed with them or with others.
- I will not attempt to invite anyone to the live video lesson. Only teachers will invite students to live lessons.
- During a live video lesson I will use the audio 'mute' function as instructed to do so by the teacher.
- During a live video lesson I will use the video function to stop the visual link when instructed to do so by the teacher.
- I agree that if I am involved in a live video session and I do not adhere to any of the rules above I will be removed from the lesson by the teacher.
- If I am removed from a lesson by a teacher, I will not be permitted to rejoin the class until the teacher or a senior member of staff has spoken with my parent/carer.

General Learning expectations

- I understand that the normal high standards of behaviour are expected of me, my interactions and engagement will be focused, polite and respectful at all times.
- I understand that this is a new way of working and that I need to focus even harder and really apply my listening skills to make the most of my learning
- I agree that messages that I post on Google Classroom and Zoom are the same as verbal communication in school and should always be positive, polite and respectful.
- I agree to always interact with any other learners in a polite and respectful manner
- I agree that I will always complete the work to the best of my ability and that I will work to the normal expectations of the school's behaviour policy in all interactions and the effort that I apply to my learning.

The School Behaviour Policy still applies