

**BRYMORE ACADEMY**

**E SAFETY POLICY**

|  |
| --- |
| **Created by:** Mark Thomas, Luke Winter |
| **Date:** January 2022 |
| **Approved by Local Advisory Board:** |
| **Review date:** January 2023 |
| **Signature of Chair of Governors**C:\Users\Julie.Vearncombe\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Jason Gunningham.jpg | **Signature of Headteacher****Shape  Description automatically generated with low confidence** |



Contents

[Introduction 3](#_Toc65420717)

[Aims and Objectives 3](#_Toc65420718)

[Staff 4](#_Toc65420719)

[Governors: 5](#_Toc65420720)

[Roles and Responsibilities: 5](#_Toc65420721)

[Headteacher and Senior Leaders: 5](#_Toc65420722)

[Roles and Responsibilities: 5](#_Toc65420723)

[Teaching and Support Staff 6](#_Toc65420724)

[Roles and Responsibilities: 6](#_Toc65420725)

[Focus 6](#_Toc65420726)

[Students and Parents/Carers 7](#_Toc65420727)

[Students 7](#_Toc65420728)

[Roles and Responsibilities: 8](#_Toc65420729)

[Mobile Phones 8](#_Toc65420730)

[Parents / Carers 9](#_Toc65420731)

[Roles and Responsibilities: 9](#_Toc65420732)

[Network Manager / Technical staff: 9](#_Toc65420733)

[Roles and Responsibilities: 10](#_Toc65420734)

[Response to a Breach of Policy 10](#_Toc65420735)

[Incident Reporting 11](#_Toc65420736)

[Inappropriate Material 11](#_Toc65420737)

[E-Safety Education 12](#_Toc65420738)

[Data Protection 13](#_Toc65420739)

[Social Media 14](#_Toc65420740)

[Use of Digital / Video Images 15](#_Toc65420741)

[Appendix 1 – Responding to an Online Incident Flowchart 16](#_Toc65420742)

[Appendix 2 – Student Acceptable Use Agreement 17](#_Toc65420743)

[Appendix 3 – Parent/Carer Acceptable Use Agreement 20](#_Toc65420744)

[Appendix 4 – Digital/Video Images Permission Form 22](#_Toc65420745)

[Appendix 5 – Staff Acceptable Use Agreement 23](#_Toc65420746)

# Introduction

New technologies have become integral to daily life whether in or outside of schools. The internet and other digital and information technologies and platforms are powerful tools as both a means of communication and in facilitating extensive access to, and sharing of, information. The School is committed to safeguarding and promoting the welfare of its students both within the school environment and outside whilst in the care of the School and this Policy intends to give direction as to how we seek to educate our students to explore their horizons by using online devices, technologies and platforms and by doing so with safety, caution and responsibility for themselves and with equal respect for others.

At Brymore Academy we recognise and value the benefits this can bring to a student’s education but remain aware that these technologies can pose threats and risks not only to the user but also to others.

**This E-Safety Policy applies:**

* **To all members of the school community including students, staff, volunteers, parents/carers and visitors when they are on site and at all times when they are using the School’s network or devices whether on site or remotely.**
* **To all students, staff and volunteers when they are off the school site for incidents which may take place out of school but are, or can be, linked to membership of the School.**

## Aims and Objectives

ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of young people and adults. Consequently, at Brymore Academy we feel the need to build in the use of these technologies to equip our students with the skills to access life-long learning and employment.

We also recognise the constant and fast paced evolution of ICT within our society. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

|  |  |  |
| --- | --- | --- |
| * Website
 | * Blogs and Wikis
 | * Gaming
 |
| * Email
 | * Instant Messaging
 | * Shopping
 |
| * Social Networking
 | * Streaming
 | * Downloading
 |
| * Online Learning
 | * Use of Mobile Technology
 | * Podcasts
 |

The School understands its responsibility to educate students in online safety; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legally compliant when using the internet and related technologies in and beyond the context of the classroom and so that they can learn to:

* Evaluate what they see online and make judgements about what they see and not automatically assume that whatever they see is true, valid, or acceptable.
* Recognise techniques used for persuasion, the techniques that are often used to manipulate others and understand that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.
* Use appropriate online behaviour and understand what acceptable and unacceptable online behaviour look like and therefore are able to recognise, and act appropriately towards, unacceptable behaviour in others.
* Identify online risks and make informed decisions about how to act.
* Know when to seek support, whether it is response to a concern, how they should act or if they are upset by something they have seen online.

Both this policy and the Acceptable Use Agreements for all students, staff and visitors found in the appendices herewith are inclusive of, but not limited to, fixed and mobile internet; technologies provided by Brymore Academy (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students, staff, and visitors, but brought onto school premises (such as laptops, mobile/smart phones, tablets, MP3 players, etc.).

Brymore Academy will deal any incidents in line with the School Behaviour and Anti-Bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of School.

# Staff

All staff and volunteers should act in accordance with the School’s Code of Conduct and be good role models in their use of ICT, the internet and mobile devices.

Online safety issues are embedded in all aspects of the curriculum and other school activities. Staff must monitor ICT activity in lessons, extra-curricular and extended school activities including in boarding time.

Staff should ensure that in using ICT in teaching, prep or other school activities students:

* understand and follow the School’s online safety rules, including those in the School’s Behaviour Policy, and the Acceptable Use Agreement.
* have an understanding of research skills and the need to avoid plagiarism and to uphold copyright regulations.

Any online safety incident is to be dealt with in accordance with the Behaviour Policy and brought to the attention of the Senior Leadership Team, who will decide how to proceed with the matter. Any safeguarding incidents should additionally be brought to the immediate attention of the DSL. The right to privacy is reduced in any circumstance where safeguarding or welfare of students may be compromised, whether this is through the School’s own network or on personally owned equipment.

## Governors:

### Roles and Responsibilities:

Governors have overall responsibility for safeguarding, promoting student welfare and well-being at the School. However, protecting students and securing their welfare is also the responsibility of all staff. The School has a Safeguarding Policy in place and its procedures must be followed where there are any matters arising from the use of the internet or of electronic devices which compromise student safety and/or welfare.

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

## Headteacher and Senior Leaders:

### Roles and Responsibilities:

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the School community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

The Headteacher and Senior Leadership Team will:

* be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
* regularly liaise with the E-Safety Co-ordinator.
* ensure that there is a clear and consistent approach for responding to incidents and maintain and implement a series of policies and procedures through which behaviour and actions can be moderated including a Safeguarding Policy, Risk Assessment Policy, Behaviour Policy and Behaviour Management Policy.
* ensure all staff are:
	+ aware of, and adhere to, the School's policies and procedures for the health, safety and welfare of students.
	+ appropriately trained in matters of online safety and are vigilant throughout the day and in boarding time for any signs of potential misuse or abuse of technology.
	+ aware of the regulations permitting and guiding the searching of electronic devices.
* provide adequate and suitable education and training for students through the curriculum and in general so that they can be better informed in the use of and potential threats/risks associated with the use of the internet and of electronic devices. Good educational provision should help students build resilience to the risks which they may be exposed to, and have the confidence and skills to face and deal with these risks.
* engage with parents to ensure that they are equally informed of the potential threats/risks associated with the use of the internet and of electronic devices and gain their support in expecting their children to be safe users of technology both in and out of school.
* set boundaries for the use of the School’s own network and devices, and for personal ICT equipment used in school, including the use of social media services both during the school day and in boarding time.
* ensure there are routine and regular monitoring systems in operation within the School’s own network and its internet provision.
* liaise and share information about concerns with local and national agencies who need to know, involving students and their parents appropriately.
* appraise Governors, through routine safeguarding reports, of education and training initiatives undertaken, any identified risks and any incidents.

## Teaching and Support Staff

### Roles and Responsibilities:

All teaching and support staff are responsible for ensuring that:

* they have read and understood the schools E-Safety Policy
* they have read, understood and signed the Staff Acceptable Use Agreement
* they report any suspected misuse or problem to the Senior Leadership Team
* they immediately report any safeguarding incidents to the DSL
* all digital communications with students/parents/carers 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 activities
* they encourage all students to understand and follow the e-safety and acceptable use policies.
* they are responsible for the security of their username and password and changing their password regularly when prompted

### Focus

When using communication technologies Brymore Academy considers the following as good practice:

* The official School email service is regarded as safe and secure and is monitored. All staff are aware that email communications are monitored.
* Staff immediately report receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
* Any digital communication between staff and students or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging or social media must not be used.
* Staff are permitted to bring in personal mobile phones and devices for their own use. Under no circumstances is a member of staff permitted to contact a student or parent using their personal device unless it is for the purpose of enhancing their duties (e.g. contacting a student with information during a school trip).
* Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.
* New staff receive information on the School’s Acceptable Use Policy as part of their induction.
* All staff must be aware of individual responsibilities relating to the safeguarding of students within the context of online safety 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 online safety activities and awareness within their curriculum areas.
* Information and training updates on online safety issues are provided.
* Staff complete Prevent Awareness Training in order to become more familiar with the signs and symptoms of extremism and appropriate responses to it.

# Students and Parents/Carers

## Students

### Roles and Responsibilities:

All Students are required to assume responsibility for their own behaviour and this extends to their use of the internet and any electronic devices. The rules applied to the use of the School’s network and its devices also apply equally to students’ own internet, communications access and relevant devices.

All students at Brymore Academy will:

* be respectful and tolerant of others being mindful of and responsible for their own welfare and that of others.
* be responsible for using the School digital technology systems in accordance with the Student Acceptable Use Policy.
* read and sign the Student Acceptable Use Agreement
* understand the importance of reporting abuse, misuse or access to inappropriate materials and know how and who to report these incidents to whilst at or outside of school
* ideally have a good understanding of research skills, the need to avoid plagiarism and uphold copyright regulations
* accept and adhere to the boundaries of use of the School’s own network and devices, or personal electronic equipment used in school, including the use of social media services and mobile telephones in the school day and during boarding time.
* know and understand the rules on the taking / using of images of others and on cyber-bullying. Any form of bulling behaviour or harassment will not be tolerated, and will be dealt with in accordance with the School’s Anti-Bullying Policy.
* 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.
* make any personal/mobile ICT equipment used on school site available as necessary for anti-virus updates and software installations, patches or upgrades as well as PAT testing.

The Education and Inspections Act 2006 permits the regulation of the behaviour of students when they are off the school site including the imposition of sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this Policy, which may take place out of school, but are linked to membership of the School.

### Mobile Phones

Brymore Academy is a boarding school and as such all students are allowed to bring personal mobile devices/phones to school. These 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. Many existing mobile technologies such as portable media players, tablets, gaming devices, mobile/smart phones are familiar to children outside of school too. These often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use.

Students must be aware that:

* all mobile devices must be turned off during lesson time.
* mobile devices can be used in social times during the school day and in boarding
* the School is not responsible for the loss, damage or theft of any personal mobile device.
* the sending of inappropriate messages between any members 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.
* the Acceptable Use Agreement relates to all use of the mobile device on or off the School wireless network.
* Failure to follow the Acceptable Use Agreement could result in a fixed length ban from using personal technology within School. Mobile phones will be handed in at the start of the day and kept in reception in case of emergencies. They will then be returned when the student leaves site.

## Parents/Carers

### Roles and Responsibilities:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Brymore Academy will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website/VLE and information about national local e-safety campaigns and literature. Parental engagement is vital to ensure that students are as safe online at home as they are in school. Recognising the boarding nature of the School and therefore the distance between school and students’ homes parents are encouraged to ask for any information and guidance if they need it.

Parents and carers will be encouraged to support the School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at School events.
* access to parents’ sections of the website and use of educational apps (e.g. MyEd).
* their children’s personal devices on site.

The School will therefore seek to provide information and awareness to parents and carers through:

* + - * Letters, newsletters, and Bymore Academy website
			* Parents/Carers evenings/sessions
			* High profile events/campaigns e.g. Safer Internet Day

## Network Manager / Technical staff:

### Roles and Responsibilities:

TheNetwork Manager/Technical Staff/Co-ordinator for ICT/Computing is responsible for ensuring:

* that the School’s technical infrastructure is secure and is not open to misuse or malicious attack.
* that the School meets required e-safety technical requirements and any Local Authority other relevant body E-Safety Policy/Guidance that may apply.
* that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
* 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/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and E-Safety Coordinator.
* filtering should be sufficient to reduce the risk, as far as possible, of students being exposed to potentially illegal or inappropriate sites.
* all users have clearly defined access rights to School technical systems and devices and are provided with a username and secure password. An up to date record of users and their usernames will be kept.
* School technical systems are managed in ways that ensure that the School meets recommended technical requirements.
* there are regular reviews and audits of the safety and security of School technical systems.
* servers, wireless systems and cabling must are securely located and physical access to these is restricted.
* Software licence logs are accurate and up to date (for installed software after 8th March 2015) and regular checks are made to reconcile the number of licences purchased against the number of software installations.

School data should generally not leave site and if it must leave site it should be encrypted. Any loss of data should be reported immediately.

The School’s ICT Support Staff have the right, on the School’s network, to change any user’s password or access rights if they deem it necessary and will report inappropriate access to the Senior Leadership Team who will, where appropriate, escalate and refer the incident to the Designated Safeguarding Lead (DSL).

# Response to a Breach of Policy

A breach or suspected breach of policy by a student, member of staff or visitor may result in the temporary or permanent withdrawal of school ICT hardware, software or services from that individual/those individuals. Any policy breach is grounds for disciplinary action in accordance with the School’s Behaviour Policy or Disciplinary Procedure as appropriate and serious policy breaches may also lead to criminal or civil proceedings.

## 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 ICT Manager and the Senior Leadership Team.

Additionally, all security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the E-Safety Coordinator.

All online safety incidents involving students should be recorded by staff on SIMS.

Any safeguarding concerns should be immediately reported to the DSL.

## Inappropriate Material

It is hoped that all members of the School community will be responsible users of digital technologies, who understand and follow School policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse. Accidental access to inappropriate materials must be immediately reported to the DSL and the Senior Leadership Team.

In the event of suspicion of deliberately accessing inappropriate material, all steps in this procedure should be followed:

* Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
* Immediately stop use of the suspected computer/mobile phone. Mobile phones should be placed onto airplane mode or turned off and confiscated.
* If content being reviewed could include images of child abuse then any investigation should not take place and it should be referred to the Police immediately. Other instances to report to the police would include:
	+ incidents of ‘grooming’ behaviour
	+ the sending of obscene materials to a child
	+ adult material which potentially breaches the Obscene Publications Act
	+ criminally racist material.
	+ other criminal conduct, activity or material.
* Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the School and the police.

**If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Responding to an Online Safety Incident Flowchart in Appendix 1.**

# E-Safety Education

ICT and online resources are increasingly used across all aspects of school life so it is essential for online safety guidance to be given to the students on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote online safety during lessons, tutorials and creative activities. Educating students on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.

At Brymore Academy we will provide a rounded approach to promoting E-Safety in the following ways:

* A planned e-safety curriculum will be provided as part of Computing/PSHRE/other lessons and will be regularly revisited.
* Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
* Students will be reminded in all lessons to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information.
* 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 and respecting other people’s information, images, etc. through discussion, modelling and activities.
* Students will be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
* Staff will act as good role models in their use of digital technologies the internet and mobile devices.
* 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 searches.
* Where students can freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
* 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 Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
* Students should be advised to immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory or threatening in nature and understand they must not respond to any such communication.
* 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 teacher/ trusted staff member, or an organisation such as Childline or Whisper.
* Whole school assemblies are also used to keep the understanding and importance of online safety current.

# Data Protection

Brymore Academy holds personal data on students, staff and other people in order to conduct 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 potential loss of sensitive information could result in media coverage and damage to the reputation of the School. In order to ensure this does not happen all staff have 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 are made aware of the risks and threats and how to minimise them.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

* fairly and lawfully processed.
* processed for limited purposes.
* adequate, relevant and not excessive.
* accurate.
* kept no longer than is necessary.
* processed in accordance with the data subject’s rights.
* secure.
* only transferred to others with adequate protection.

Brymore Academy ensures that:

* the minimum amount of personal data necessary is held to enable it to perform its function and it will not be held for longer than necessary for the purposes it was collected for.
* every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
* all personal data is fairly obtained and lawfully processed.
* there is a Data Protection Policy.
* it is registered as a Data Controller for the purposes of the Data Protection Act (DPA).

All staff must:

* ensure that any school information accessed from personal equipment or removable media equipment is kept secure.
* log off before moving away from a computer during the normal working day to prevent unauthorised access.
* ensure the accuracy of any personal, sensitive, confidential and classified information disclosed or shared with others and that it is not disclosed to any unauthorised person.
* ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.
* not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
* keep screen displays out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.
* ensure hard copies of data are securely stored and disposed of after use.

When personal data is stored on any portable computer system, memory stick or any other removable media:

* the data must be encrypted and password protected.
* the device must be password protected.
* the device must offer approved virus and malware checking software.
* the data must be securely deleted from the device, in line with School policy (below) once it has been transferred or its use is complete.

# Social Media

All Schools have a duty of care to provide a safe learning environment for students and staff. The School could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the School liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

**Brymore Academy staff should ensure that:**

* no reference should be made in social media to students, parents/carers or School staff.
* they do not engage in online discussion on personal matters relating to members of the School community.
* personal opinions should not be attributed to the School or Local Authority.
* security settings on personal social media profiles are regularly checked to minimise any risk of loss of personal information.
* students are informed and educated 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.

# Use of Digital / Video Images

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 in the public media.

The School will comply with the Data Protection Act and request parents’/carers’ 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.

Parents/carers are requested to sign the permission form in Appendix 4 to allow the School to take and use images of their children and for the parents/carers to agree.

In accordance with guidance from the Information Commissioner’s Office, parent /carers are welcome to take videos and digital images of their children at School events for their own personal use (as such use in not covered by the Data Protection Act). 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 parents/carers comment on any activities involving other students in the digital/video images.

Digital images are easy to capture, reproduce and publish and, therefore, misuse. 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) and staff, the School permits the appropriate taking of images by students and staff with school equipment.

# Appendix 1 – Responding to an Online Incident Flowchart



# Appendix 2 – Student Acceptable Use Agreement

**Student Acceptable Use Agreement**

**I understand that I must use Brymore Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.**

**For my own personal safety:**

* I understand that Brymore Academy 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)
* I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

* I understand that Brymore Academy 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 Brymore Academy’s systems or devices for on-line gaming, internet shopping or file sharing unless I have permission of a member of staff to do so and at the times that are allowed.

**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 Brymore Academy** **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 in accordance with the agreed policies and 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 Brymore Academy 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 a fixed length ban from using personal technology within school hours, loss of access to the School network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

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

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

Name of Student

Tutor Group

Signed

Date

# Appendix 3 – Parent/Carer Acceptable Use Agreement

**Parent/Carer Acceptable Use Agreement**

Digital technologies have become integral to the lives of children and young people, both within Schools and outside School. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

• That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• That Brymore Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Brymore Academy will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the School expectations of the young people in their care. Our E-Safety Policy is also available on the Brymore Academy Website.

Parents are requested to sign the permission form below to show their support of the School in this important aspect of the School’s work.

**As the parent / carer of the above students, I give permission for my son to have access to the internet and to ICT systems at Brymore Academy.**

I know that my son has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help him understand the importance of safe use of technology and the internet – both in and out of School*.*

I understand that Brymore Academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the School cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son’s activity on the ICT systems will be monitored and that Brymore Academy will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my son to adopt safe use of the internet and digital technologies at home and will inform Brymore Academy if I have concerns over my child’s e-safety.

**Parent/Carer Name**  **Student Name**

**Signed** **Date**

# Appendix 4 – Digital/Video Images Permission Form

**Digital / Video Images Permission Form**



**PARENTAL CONSENT**

**Photography**

As parent/guardian of ......................................................................................................

I  **consent /  do not consent** (please tick appropriate box) to photographs of him to be used for selected purposes relating to Brymore Academy.

**Please note, if you do not consent then we cannot guarantee your child will be included in whole school photos and photos taken at other commemorative occasions.**

Signed Date

**PLEASE SIGN AND RETURN THIS SLIP TO BRYMORE ACADEMY IMMEDIATELY**

# Appendix 5 – Staff Acceptable Use Agreement

**Staff Acceptable Use Agreement**

New technologies have become integral to the lives of children and young people in today’s society, both within Schools and in their lives outside School. The internet and other digital information and communications technologies are powerful tool which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

* That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* That Brymore Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* That staff are protected from potential risk in their use of ICT in their everyday work.
* Brymore Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

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

**For my professional and personal safety:**

* I understand that Brymore Academy will monitor my use of the ICT systems, email and other digital communications.
* I understand that the rules set out in this agreement also apply to use of Brymore Academy ICT systems (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 Brymore Academy ICT 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.

28

**I will be professional in my communications and actions when using Brymore Academy 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 Brymore Academy’s policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Brymore Academy website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
* I will only use chat and social networking sites in School in accordance with the Brymore Academy policies.
* I will only communicate with students and parents/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 and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the School:**

* When I use my mobile devices (PDAs/laptops/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 School equipment. I will also follow any additional rules set by the School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
* I will not use personal email addresses on the Brymore Academy ICT systems.
* 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 Brymore Academy 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 School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
* I understand that data protection 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 Brymore Academy. I understand that this Acceptable Use Policy applies not only to my work and use of Brymore Academy ICT equipment in School, but also applies to my use of Brymore Academy l ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Brymore Academy. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities the involvement of the police.**

I have read and understand the above and agree to use the Brymore Academy ICT 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