BRADING CE CONTROLLED PRIMARY SCHOOL

E-SAFETY

(INCORPORATING THE SOCIAL MEDIA POLICY & PHOTOGRAPHIC IMAGES OF CHILDREN POLICY)

A STATEMENT OF POLICY

Reviewed by Governors

Date Agreed: **March 2018**

Review Date: **March 2019**

Signed: _____

Brading CE Primary School E-Safety Policy

Introduction

Technology and communications are rapidly changing and becoming more sophisticated, with this change comes new ways of being unsafe and feeling threatened. E- Safety has become a very important issue that is essential to address in school throughout different areas of the curriculum, to ensure that all children and adults remain safe and in control when using technology. This could be either computers and having access to the internet, or through mobile telephones.

1. Aims

We aim to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Stay in control and keep personal information private.
- How to take the necessary measures to block and delete accounts, messages and people.

2. Roles and Responsibilities

All the adults that are involved in the life of the school; whether governors, teaching staff, support staff, technicians , community have roles and responsibilities that are associating with E-Safety as well as all pupils that come into contact with computers.

Governors

The Governors are responsible for the approval of the E-Safety Policy and reviewing the effectiveness of it regularly. Regular meetings and information will be provided to the Governors so they are able to make the correct recommendations, they will also be able to carry out regular monitoring of E-Safety incident logs when required.

Headteacher and Senior Leadership

The Headteacher is responsible for ensuring the safety, including E-Safety, of the members of the school community. Although the day to day managing of E-Safety will be delegated to the E-Safety Co-ordinator.

The Headteacher and Senior Leadership Team are responsible for ensuring that all staff and the E-Safety Co-ordinator receive correct and suitable Continuing Professional Development (CPD).

The Headteacher and Senior Leadership Team will ensure that there is a system in place to monitor the usage of internet and other technologies and that the person who carries out the internal E-Safety monitoring receives support and is also monitored. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and Senior Leadership Team will ensure that they receive regular updates and reports from the E-Safety Co-ordinator.

The Headteacher and another member of the Senior Leadership Team are to ensure they know the correct procedures that need to be followed when a serious allegation has been made by a child or one that is in regards to a member of a staff.

E-Safety Co-ordinator

The E-Safety Co-ordinator will take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents.

The E-Safety Co-ordinator will ensure that all staff is aware of the procedures that need to be followed in the event of an e-safety incident taking place and will provide training and advice for all staff.

The E-Safety Co-ordinator will liaise with the Local Authority and liaise with school ICT technical staff.

The E-Safety Co-ordinator will receive reports of E-Safety incidents and creates a log of incidents to inform future e-safety developments.

The E-Safety Co-ordinator will meet regularly with Governors to discuss current issues, review incident logs and filtering /change control logs and reports regularly to Senior Leadership Team.

Technical Staff

The Network Manager /ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- the school meets the e-safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- he/ she keeps up to date with relevant E-Safety technical information and guidance in order to carry out their role effectively.
- monitoring software/ systems are implemented and up dated regularly.

Teaching and Support Staff

Teaching and Support Staff are responsible for -

- Ensuring they stay up to date with current E-Safety matters and policies and practice.

- They read, understand and carry out the Acceptable Use Policy (AUP).
- They report any misuse or problems to the E-Safety Co-ordinator/ Headteacher for further investigation.
- That any digital communications with pupils (email, Learning Platform) should be strictly professional and only carried out using school systems.
- That E-Safety issues are embedded throughout the curriculum.
- That pupils follow the AUP and E-Safety policy.
- Being are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

Child Protection Officer

The Child Protection Officer needs to ensure that they are fully trained in E-Safety issues and are aware that there serious child protection issues could occur due to-

- Cyber- bullying
- Sharing of personal data
- Prevent duty
- Child Sexual Exploitation
- Female genital Mutilation
- Forced Marriages
- Honour Based Violence
- Inappropriate online conduct with adults/ strangers
- Potential or actual incidents of grooming

Pupils/ Students

Pupils and students are responsible for-

- Knowing and acting accordingly to the school's AUP.
- Knowing the importance of reporting abuse, misuse or access to inappropriate materials and know how to report them.
- Knowing the policy on mobile phones, digital cameras and other hand held devices and to realise these can be used for cyber-bullying.
- Understanding that the E-Safety policy also covers their actions out of school, if related to their membership of the school.

Parents/ Carers

Parents and carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. They must be aware of the schools AUP and agree to it.

3. Education

All children will receive planned E-Safety lessons throughout ICT/ P.S.H.E lessons, these lessons will be regularly revisited and revised to suit the new technologies in and out of school. Key messages will be delivered through a variety of assemblies to ensure all children are aware of the matter. They will also be made aware to question the validity of the information they find online.

Parents will be able to attend regular E-Safety meetings, where they will also have the chance to ask questions regarding E-Safety. They will also receive information via parents' evenings and newsletters.

All staff will receive regular training regarding E-Safety and an audit of their E-Safety needs will be carried out. All new staff will receive E-Safety training as part of the induction process, ensuring they are fully aware and understand the E-Safety policy and the AUP. The E-Safety Co-ordinator will be able to attend to regular updates provided by the Local Authority or other training schemes and report back to staff any new issues that they need to be aware of. The E-Safety Co-ordinator will provide guidance for any member of staff that seeks it.

Governors will attend regular meetings, which will provide information about E-Safety.

4. Technical

Brading CE Primary School receives a filtered broadband service through the broadband connectivity. This service is intended to stop users from accessing any material that would be regarded as inappropriate for the learning environment or illegal.
The service is provided by RM safety net and this allows for the service to be flexible, so the school can have ownership of what else needs to be filtered as technology advances.
The school filtering system has been designed to educational objectives and has been approved by RM safety net.
All staff and pupils will be made aware that there is also a monitoring system in place and any online activity can be traced. The person responsible for monitoring this will also be monitored by the Headteacher to ensure that this is being done effectively and correctly. A member of SLT will also aid in the monitoring of the member of staff who is responsible for it.

All personal data will be stored accordingly to the Personal Data Act 1998. Staff must use personal data on secure password protected machines and other devices, ensuring that they 'log off' at the end of any session. This will then minimise any chance of the data being seen by others. Any personal data that is stored on a USB device also needs to be password protected an encrypted. Devices must have virus and malware checking software. Any data must be securely deleted from any devices.

5. Curriculum

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

- In lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, eg using search engines, 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 during (eg weapons, which could be part of a study on the Roman Army) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should have clear reasons to support the need of these websites. Requests for website release should be made on an appropriate request pro-forma.

- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.

Communications

This is an area which is rapidly developing and will need to be constantly revisited as technology advances and changes. Brading CE Primary School recognises that different communications can have the potential to enhance learning and therefore can be a powerful tool. But we are also aware of the risks that may come with these too in regards to E-Safety.

Below is a table which outlines the how these communication devices are to be used by both staff and children at school. Some applications are permitted at certain times, but are strictly for education purposes. If there are any queries/ uncertainty please seek the guidance of the E-safety co-ordinator

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						
Taking photos on mobile phones or other camera devices			x					
Use of hand held devices eg PDAs, PSPs				x				x
Use of personal email addresses in school, or on school network	x						x	
Use of school email for personal emails		x					x	
Use of chat rooms / facilities				x				x
Use of instant messaging		x						x
Use of social networking sites				x				x

Use of blogs		x					x	

Use of Digital Video and Images

The developments of digital images and videos have significant benefits within the curriculum and enhance learning. Image and videos can either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/ video is posted on the internet that it will remain there forever. This could cause harm or embarrassment in the future.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- Staff are allowed to take digital / video images to support educational purposes, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken that when capturing images/ videos that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils or the school into disrepute.

- Pupils full names will not be used anywhere on the website or in blogs and particularly not associated with photographs on there.

- Written permission must be obtained from the parent or carer of any child before pictures are published on the website. Written permission is provided for every child that starts the school to indicate whether the parent or carer allows their child to be photographed.

- Brading C of E Primary School will always comply with the Data Protection Act 1998 in regards to digital images and videos.

Unsuitable Use, Sanctions and Reporting (Also See Appendix 1 & 2)

Use ctions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Use shall not visi ternet site nake, pos dov oad, upl , data tra er, cor unicate or s on, ma al, ren ks, pro sals or cor ents that cor n or rela to:	child sexual abuse images				x	x
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation				x	x
	adult material that potentially breaches the Obscene Publications Act in the UK				x	x
	criminally racist material in UK				x	x
	pornography				x	x
	promotion of any kind of discrimination				x	
	promotion of racial or religious hatred				x	
	threatening behaviour, including promotion of physical violence or mental harm				x	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				x	
Usi school systems to run a private business					x	
Use stems, applications, websites or other me nisms that bypass the filtering or other saf ards employed by SWGfL and / or the school					x	
Up ding, downloading or transmitting commercial sof re or any copyrighted materials belonging to thi arties, without the necessary licensing per sions					x	
Rev ing or publicising confidential or proprietary inf ation (eg financial / personal information, dat ses, computer / network access codes and pas ords)					x	

Cre har	ng or propagating computer viruses or other ul files				x	
Car net cau the	ng out sustained or instantaneous high volume rk traffic (downloading / uploading files) that network congestion and hinders others in se of the internet				x	
On	e gaming (educational)	x				
On	e gaming (non educational)				x	
On	e gambling				x	
On	e shopping / commerce				x	
File	aring				x	
Use	social networking sites				x	

The previous table outlines what activities are acceptable and unacceptable for both staff and pupils. All users of the computers will be made aware of what is acceptable or not by the AUP. If unacceptable use is carried out the correct sanctions will be in place and the reporting of these offences is outlined.

It is expected that all users will be responsible and safe users of ICT, who understand the policy and work within it. However, at times an infringement of the policy may occur whether through carelessness or, very rarely, deliberately.

If any apparent or actual misuse appears to involve illegal activity ie,

- child sexual abuse images;
- adult material, which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials.

The correct reporting procedure is in place and all staff are aware of who to speak to in the first instance. This being, speaking to the E-Safety Co-ordinator who will then investigate the matter. If the matter is of a serious nature then either the Child Protection Officer or the Headteacher will be informed, who will take the matter further.
All children will be made aware of the importance to report any incident to either an adult at school that they can trust or the ' Report Abuse' button that is present on the school website, regarding any incidents that may occur outside of school.

If an incident has occurred due to carelessness, which will be more likely the case, this will to be investigated and the correct sanctions will be implemented. All users within the school are aware that there is a monitoring system that is in place and is sensitive enough to pick up slight infringements regarding; cyber-bullying, searching for inappropriate content etc.
The following table indicates how different offences will be dealt with in regards to both pupils and staff. In all cases the Headteacher when notified will decide what action to take and whether the incident needs further action, e.g. reporting to police, Local Authority.

Students / Pupils (Also see Appendix 1& 2)

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x			x	x		
Unauthorised use of non-educational sites during lessons		x			x	x	x	
Unauthorised use of mobile phone / digital camera / other handheld device		x			x	x	x	
Unauthorised use of social networking / instant messaging / personal email		x		x	x	x	x	
Unauthorised downloading or uploading of files		x		x	x	x	x	
Allowing others to access school network by sharing username and passwords		x		x	x	x	x	
Attempting to access or accessing the school		x			x	x	x	

network, using another student's / pupil's account								
Attempting to access or accessing the school network, using the account of a member of staff		x			x	x	x	
Corrupting or destroying the data of other users		x				x	x	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x	x		x	x	x	
Continued infringements of the above, following previous warnings or sanctions		x	x		x	x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x			x	x		x
Using proxy sites or other means to subvert the school's filtering system		x		x		x		x
Accidentally accessing offensive or pornographic material and failing to report the incident		x		x			x	
Deliberately accessing or trying to access offensive or pornographic material		x	x	x		x		

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x					x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	x	x	x		x	x	x	x
Unauthorised downloading or uploading of files	x	x				x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x					x		
Careless use of personal data eg holding or	x	x	x			x		x

transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules		x	x					x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x						x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x	x	x				x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x	x			x	x	x
Actions which could compromise the staff member's professional standing		x				x		
Actions which could bring the school into disrepute or breach the integrity of the		x	x					x

ethos of the school								
Using proxy sites or other means to subvert the school's filtering system		x	x			x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x				x		
Deliberately accessing or trying to access offensive or pornographic material		x	x				x	x
Breaching copyright or licensing regulations		x				x		
Continued infringements of the above, following previous warnings or sanctions		x	x					x

Communications Technologies

- **Mobile Phones-**The use of mobile phones will not be permitted during lessons or formal school time by staff or pupils. This excludes occasions when staff may need to use mobile phones, for example on school trips, or as part of a demonstration in a lesson. Staff may use their mobile phones in the staff room outside of formal school time but they must be switched off/on silent and not used for personal reasons during the time staff are with children.
- **School Website-**The school website is maintained and kept up to date by the Headteacher, the IT Technician and administration staff. The Headteacher ensures that the content on the school website is accurate and appropriate to the needs of the school community. No personal information about any member of the school community will be published on the website.
- **Social Networking-**The use of public online chat rooms, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the e-safety of the pupils. Thus public social networking sites and newsgroups will be blocked and filtered. Pupils are advised not to place personal photos on any social network space. Pupils are advised on security and encouraged to set passwords and deny access to unknown individuals. Pupils are advised never to agree to meet someone they

have met on a social networking site. Should pupils have any concerns about social networking sites or chat rooms, they are advised that they must tell an adult.
Staff must not publish children's surnames on school social media sites. Only children whose parents have given specific written consent may be posted on school social media sites. When posting on social media sites such as Facebook, staff must not give details of exact locations where children can be found for events outside of usual school days and times.

- **Email-**Curriculum activities that involve the use of email will be delivered through email programmes that are controlled by the school and only use email accounts that are approved by the school.
  The use of individual pupil personal accounts will not be permitted through the school system.
  The official school email service may be regarded as safe and secure and is monitored.
  Users need to be aware that email communications may be monitored.
  Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
  Any digital communication between staff and pupils 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 public chat/social networking programmes must not be used for these communications.
  Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Responding To Incidents of Misuse

All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school E-safety Policy. It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless, irresponsible or, very rarely, deliberate misuse. The Headteacher will ensure that the E-safety Policy is implemented and compliance with the policy monitored. If members of staff suspect that misuse might have taken place, they should be referred to the Headteacher. It is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

6. **Monitoring and Review** and **Policy Ownership**

Working with Parents
Our school seeks to work in partnership with parents to provide effective
E-Safety. Parents need to know that the school's E-Safety programme will complement and support their role as parents and that they can be actively involved in the determination of the school's policy.

This policy has been reviewed through consultation with the subject co-ordinator and the school's Senior Leadership Team (SLT) a draft reviewed policy has then been distributed to all staff for consultation. A final draft has then been presented to the Governors' Leadership and Management Committee for further consultation. The final policy has then been presented to the Full Governing Board and upon their ratification notification has been given to the parents (through the newsletter) that it is available for inspection and comment.

The timing of this process and next review is as outlined below:

Date of next review: March 2019

(If at any time circumstances or situations should change in this subject area the policy will be reviewed earlier)

This Policy Should be read in conjunction with the School's Safeguarding and Child Protection Policy

Appendix 1

E-Safety Risks & Issues

E-safety risks and issues can be roughly classified into three areas: content, contact and conduct. The following are basic examples of the types of e-safety risk and issues that could fall under each category.

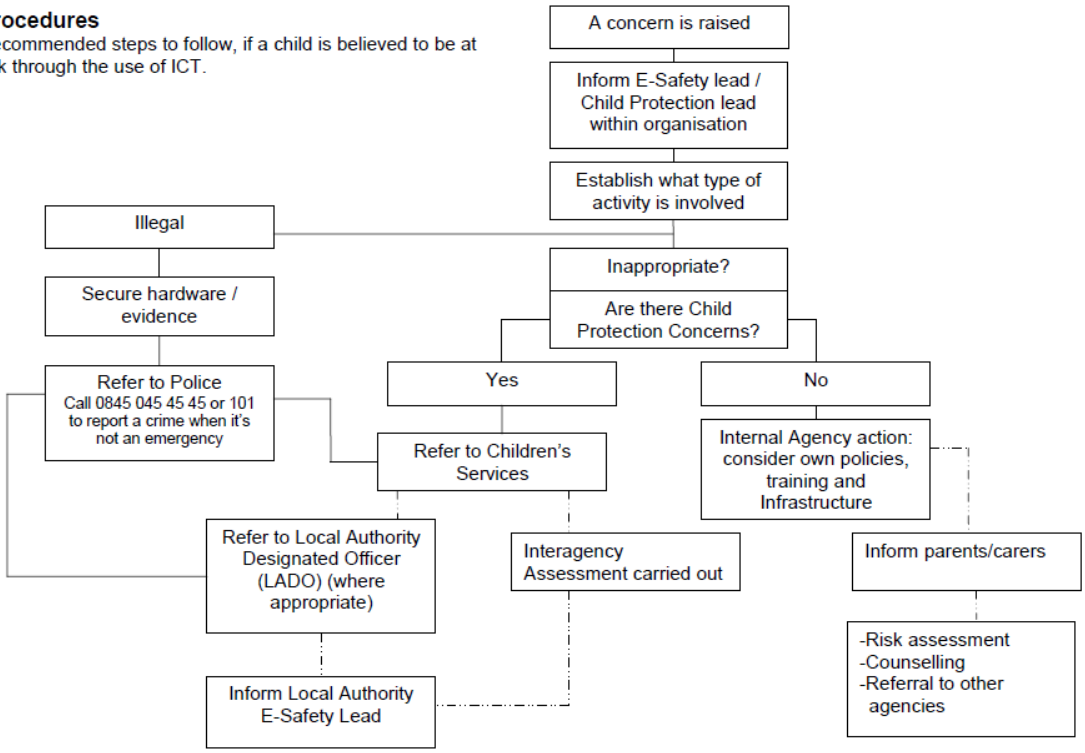
	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/ advice

DSCF, 2008 - Safer Children in a Digital Word: The report of the Byron Review

Appendix 2

Hampshire, Isle of Wight, Portsmouth & Southampton 4LSCB
E-Safety Strategy

Procedures
Recommended steps to follow, if a child is believed to be at risk through the use of ICT.



Appendix 3

Dear Parent/Carer,

As discussed on the parent information evening, Brading Primary School uses Tapestry as a way of recording the learning through the day. Although most pre-schools have transferred the Tapestry accounts to us, as part of our e-safety we need your consent for your child's photo being used on Tapestry, for your child to be included in a group observation and to agree **not** to download any photo (for example, putting them onto Facebook). Please tick the boxes and sign below. Please include your email address again and you have the option for a second email address if you have another family member who would enjoy following your child's progress. Once we have received this form we will send you a link to change your password and then your child's Tapestry account will be available for you to view. If you have any concerns, please see a member of staff.

Child's Name……

Main email address for Tapestry……

Relationship to child……

Second email address for Tapestry (optional)……

Relationship to child……..

☐ I give permission for my child's photo to be uploaded onto Tapestry

☐ I give permission for my child's photo to be used in group observations

☐ I confirm that I, and members of my family, will not use, download or reproduce any photos from Tapestry

Signed……

Date……

SOCIAL MEDIA

Statement of intent

Brading C of Controlled Primary understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

We are committed to:

- Encouraging the responsible use of social media in support of the school/academy's mission, values and objectives.
- Protecting our pupils from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.
- Arranging e-safety meetings for parents.

This policy should be read in conjunction with the school's Safeguarding and Child Protection Policy.

1. Key roles and responsibilities

1.1. The Governing Board has overall responsibility for the implementation of the Social Media Policy and procedures of Brading C of Controlled Primary

1.2. The Governing Board has responsibility for ensuring that the Social Media Policy, as written, does not discriminate on any grounds, including but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.

1.3. The governing board has responsibility for handling complaints regarding this policy as outlined in the school's Complaints Policy.

1.4. The headteacher will be responsible for the day-to-day implementation and management of the Social Media Policy and procedures of Brading C of E Controlled Primary

1.5. Staff, including teachers, support staff and volunteers, will be responsible for following the Social Media Policy and for ensuring pupils do so also. They will also be responsible for ensuring the policy is implemented fairly and consistently in the classroom.

1.6. Parents and carers will be expected to take responsibility for the social media habits of their child/children at home.

1.7. Parents and carers will be expected to promote safe social media behaviour.

2. The school's E-safety Lead is Mrs B Gilbert and Network Manager is Mrs D Stubbs

3. Definitions

3.1. Brading C of E Controlled Primary defines "social media" as any online platform that offers real-time interaction between the user and other individuals or groups including but not limited to:

- Blogs.
- Online discussion forums, such as netmums.com.
- Collaborative spaces, such as Facebook.
- Media sharing services, such as YouTube.
- 'Micro-blogging' applications, such as Twitter.

3.2. Brading C of E Controlled Primary defines "cyber bullying" as any use of social media or communication technology to bully an individual or group.

3.3. Brading C of E controlled defines "members of the school community" as any teacher, member of support staff, pupil, parent/carer of pupil, governor or ex-pupil.

4. Training of staff

4.1. At Brading C of E Controlled Primary, we recognise that early intervention can protect pupils who may be at risk of cyber bullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils.

4.2. Teachers and support staff will receive training on the Social Media Policy as part of their new starter induction.

4.3. Teachers and support staff will receive regular and on-going training as part of their development.

5. Pupil Expectations

5.1. Pupils are responsible for following the school rules and will be expected to follow requests from teachers.

6. Social Media Use - Staff

6.1. Teachers may not access social media during lesson time, unless it is part of a curriculum activity

6.2. Teachers may use social media during their break times.

6.3. Members of staff should avoid using social media in front of pupils.

6.4. Members of staff **must not** "friend" or otherwise contact pupils or parents/carers through social media.

6.5. If pupils or parents/carers attempt to "friend" or otherwise contact members of staff through social media, they should be reported to the headteacher.

6.6. Members of staff should avoid identifying themselves as an employee of Brading C of E Controlled Primary on social media.

6.7. Members of staff **must not** post content online which is damaging to the school or any of its staff or pupils.

6.8. Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal.

6.9. Teachers or members of staff must not post any information which could identify a pupil, class or the school.

6.10. Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.

6.11. Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.

6.12. Members of staff should be aware that if their out-of-work activity brings into Brading C of E Controlled Primary disrepute, disciplinary action will be taken.

6.13. Members of staff should regularly check their online presence for negative content via search engines.

6.14. Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.

6.15. Members of staff should not leave a computer or other device logged in when away from their desk, or save passwords.

6.16. Staff members should use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

7. Social Media Use – pupils and parents/carers

7.1. Pupils may not access social media during lesson time, unless it is part of a curriculum activity.

7.2. Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.

7.3. Pupils and parents/carers must not attempt to "friend" or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to Mrs B Gilbert.

7.4. If members of staff attempt to "friend" or otherwise contact pupils or parents/carers through social media, they should be reported to the headteacher.

7.5. Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.

7.6. Pupils and parents/carers must not post content online which is damaging to the school or any of its staff or pupils.

7.7. Pupils at Brading C of E Controlled Primary must not sign up to social media sites that have an age restriction above the pupil's age.

7.8. If inappropriate content is accessed online on school premises, it must be reported to a teacher.

8. Blocked content

8.1. At Brading access to social media sites on the school network is blocked by RM SafetyNet web filtering.

8.2. Attempts to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.

8.3. Inappropriate content which is accessed on the school computers should be reported to Mrs D Stubbs so that the site can be blocked.

8.4. Requests may be made to access erroneously blocked content to Mrs D Stubbs

8.5. The final decision on whether access should be granted to a site will be made by Mrs B Gilbert.

9. Cyber bullying

9.1. At Brading C of E Primary cyber bullying is taken seriously.

9.2. Incidents of cyber bullying will be dealt with and reported along the same chain as the Anti-Bullying Policy.

9.3. Staff members should never respond or retaliate to cyber bullying incidents. Incidents should instead be reported as inappropriate, and support sought from their line manager or senior staff member.

9.4. Evidence from the incident should be saved, including screen prints of messages or web pages, and the time and date of the incident.

9.5. Where the perpetrator is a current pupil or colleague, most cases can be dealt with through the school's own disciplinary procedures.

9.6. Where the perpetrator is an adult, in nearly all cases, a senior staff member should invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.

9.7. If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.

9.8. If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school should consider contacting the police.

9.9. As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PSHE.

10. Be SMART online

10.1. We encourage pupils to take a SMART approach to social media behaviour:

- **Safe** – Do not give out personal information, or post photos of yourself to people you talk to online. Follow age restriction rules.
- **Meeting** – Do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online.
- **Accepting** – We advise that pupils only open emails and other forms of communication from people they already know.
- **Reliable** – We teach pupils about the dangers of believing everything they see online.
- **Tell** – We encourage pupils to tell a teacher, parent or carer if they see anything online that makes them feel uncomfortable.

Appendix 1 – Blocked content access form

Blocked website content access request form

Teacher name:

Full URL:

Site content:

Reasons:

Risks:

Approved	Reason:
☐ Yes ☐ No	

Appendix 2 – Inappropriate content report form

Inappropriate website content report form
Teacher name:
Full URLs:
General site content:
Nature of inappropriate content:
Safeguarding issue?
Site blocked (Date):

Appendix 4

Contact details for social networking sites

Social networking site	Useful links
Ask. Fm	Terms of service Safety tips
BBM	Rules and safety
Facebook	Rules Report to Facebook Safety Centre
Instagram	Rules Report to Instagram Safety Centre
Kik Messenger	Rules Report to Kik Help Centre
Snapchat	Rules Report to Snapchat Safety tips for parents
Tumblr	Rules Report to Tumblr If you email Tumblr, take a screenshot as evidence and attach it.
Twitter	Rules Report to Twitter
Vine	Rules Contacting Vine and reporting
YouTube	Rules Report to YouTube Safety Centre

PHOTOGRAPHIC IMAGES OF CHILDREN

1. Introduction

This document provides guidance on the appropriate use of images of children in education. It covers still, video and electronic photographic images wherever they are used.

Establishments need to make full and proper use of photographic images while meeting the law and preserving the safety of children. Concerns focus on issues around rights of privacy, child protection and copyright ownership. These guidelines address these issues and give advice on good practice.

2. Typical Uses of Photographs

- Key skills for PE.
- Video Based Learning Project in PE
- Performing arts including dance and movement, concerts, drama performances, parent evenings.
- Sports days and sports fixtures and the use of photographic equipment by parents and carers and children from other schools.
- Media including newspapers and television especially when some editors require children's names when publishing photographs.
- Displays in the establishment of children's activities.
- Publications by the establishment and by the Isle of Wight Council.
- Establishment and IWCC web-sites.
- Staff training and professional development activities.
- Site security.

3. Governing Board

The Governing Board should formally adopt these guidelines as policy and good practice.

Ensure that the child protection and /or health and safety governor are aware of and support the policies and procedures.

4. Ownership

Human Rights legislation and the Data Protection Act 1998 give people new rights and it is the right to 'privacy' that is the issue when using photographs. The Council and establishments must take steps that respect the rights of people in photographs.

The Copyright, Designs and Patent Acts 1988 moved the ownership of copyright to the photographer (or their employer) and away from the person commissioning and paying for the photographs, unless there is an agreement otherwise.

5. Good Practice

The following advice represents good practice in the use of photographic images involving children.

1. When taking a picture the establishment must obtain the consent of the person in the picture or from their parent or carer.
2. If using a photo from the media or commissioning a photograph, have a signed agreement.

3. Use the image in its intended context. Examples of this not happening are:
   - when a picture taken by a national newspaper of a child accepting an award was used by the National Front in a story with a completely different story angle.
   - When a photo of the public boarding a bus to launch a rural transport initiative is used to illustrate a story attacking rural transport shortages.
4. Follow the commitment made in the consent forms:
   - not to use the photograph out of context;
   - not to use the photograph to illustrate sensitive or negative issues.
5. When photographing children:
   a. Ensure that parents and carers of young people have signed and returned the establishment consent form for general photography.
   b. Ensure all children are appropriately dressed.
   c. Avoid images that only show a single child with no surrounding context of what they are learning or doing.
   d. Photographs of three or four children are more likely to also include their learning context.
   e. Do not use images of a child who is considered very vulnerable, unless parents / carers have given specific written permission.
   f. Avoid naming young people. If one name is required then use the first name only where possible.
   g. Use photographs that represent the diversity of the young people participating.
   h. Report any concerns relating to any inappropriate or intrusive photography to the head teacher.
   i. Remember the duty of care and challenge any inappropriate behaviour or language.
   j. Do not use images that are likely to cause distress, upset or embarrassment.
6. Regularly review stored images and delete unwanted material.

6. Parental Permission

Use of images of children requires the consent of the parent / carer. Permission should always be obtained, when a child joins the establishment. The form covers the establishment and using the photographs in publications and on web-sites. Each year as part of a standard communication, ask parents if they wish to change their permission. If they do, encourage them to contact the head teacher.

When a parent does not agree to their child being photographed, the head teacher must inform staff and make every effort to comply sensitively.

For example, if a child whose parents have refused permission for photography is involved with a sports event, e.g. a football match, it may not be appropriate to photograph the whole team. Careful liaison with parents is therefore essential. With discussion it may be possible to agree other options. The parent may accept a team photograph if names are not published or they may be prepared to relent if it affects the whole team.

When photographic images are transmitted or shared beyond the establishment e.g. television broadcasts, images on intranet sites, specific permission should be obtained.

7. Inter-School Fixtures

Apply these guidelines to inter-school events. If a vulnerable child is involved, it will be necessary to liaise with a member of staff from the other establishment so that they are aware of the wishes of the parents or carer of the child and seek the co-operation of the parents of the opposing team.

8. Teacher Training and Portfolios

During teacher training and with newly qualified staff, colleagues need to compile portfolios with photographs of children during lessons. Staff should act responsibly in compiling these images. A member of the management team may wish to oversee the compiled images as part of the management process and consider their appropriateness.

9. Displays in Schools

Still photographs shown on displays and video clips available during open / parents' evenings should depict children in an appropriate way. They should not display images of children in inappropriate or revealing clothing so appropriate levels of integrity and decency are maintained. Do not use photographs or images likely to cause embarrassment.

10. Parents Evenings, Concerts, Presentations

To allow the appropriate recording of children's images, parents, carers and visitors will be reminded of their duty to support the safeguarding of all children- only if permission has been given by all parents in school to allow them to photographed etc. If not then no permission will be given to parents to use cameras to photograph children at school events, including mobile phone cameras.

The school will take still and video images of events which will be shared with the relevant parents, if agreed permission is received from all parents.

11. Children Photographing Each Other

This practice can occur extensively during offsite activities particularly during residential periods. Staff should maintain the supervision and management control. There may be incidents where children take inappropriate photographs, perhaps showing friends and other children inappropriately dressed. Staff should endeavour to discourage this practice, but ultimately parents are responsible for monitoring their child's use of cameras and subsequent use of their images involved.

12. Newspapers

Several scenarios can occur:

1. Team photographs:

- If a parent is not happy to have a child's name printed on a photograph then consideration could be given to publishing the photograph with no names. The head teacher / manager should make every effort to ensure, in conjunction with the newspaper editors, that this occurs.
- If parents of a child have indicated that the child is vulnerable and should not have a photograph printed then a team photograph may not be appropriate.
- Publication can occur when everyone is prepared to allow team photographs and full names are to be published.

2. Photo opportunities:

- When an establishment invites a newspaper to celebrate an event, the head teacher should make every effort IN ADVANCE to ensure that the newspaper's requirements can be met.

- Almost without exception, this means the paper will prefer to publish the full names of anyone in a photograph they print. The only exception to this might be (as above) in a larger group shot (e.g.: a group of more than 10 children).
- However newspapers usually prefer to work with smaller groups of children – e.g.: three or four – and for this number names would definitely be required.
- It is not acceptable to invite a newspaper to take photographs and then refuse to provide any names. Newspapers will not print anonymous photographs. Establishments must give thought to this beforehand – and parental permission / opinion must be their key guidance.
- This might mean offering only those children whose parents are happy for publication of photographs and names for inclusion in any photo opportunities.
- If this is not possible – for instance because a specific group of children have achieved something, and parental permission re. the publication of full names is withheld for one or more of the group - it might be possible to negotiate a 'first names only' agreement with the newspaper.
- Otherwise establishments must be prepared to forego newspaper publicity.

13. Use of Internet / Intranet Sites

Many establishments will have an internet / intranet facility. The site manager should know good practice and ensure that the establishment only uses appropriate images that follow this guidance. For example, if a child has successfully completed a gymnastics award, it would be appropriate to show the child in a tracksuit rather than leotard.

14. Mobile Phones

Only mobile phones that are supplied by the school can be taken into changing rooms, with the exception of the group leader who has DBS clearance. Mobile phones with photographic facilities are not permitted to be taken into toilets with children present at any time. The schools only have mobile phones that have no photographic facilities.
Pupils who bring mobile phones into school must hand them in to their class teacher for the duration of the school day.

This policy should be read in conjunction with the school's Safeguarding & Child Protection Policy

Stage 1 Equality Impact Assessment – Initial Screening

Assessor(s) Name(s):	Bev Gilbert
School:	Brading Primary School
Date of Completion:	1st March 2015

Name of Policy
Photographic Images of Children Policy

The Aims, Objectives and Expected Outcomes:
This policy provides guidance on the appropriate use of images of the children within our care at Brading Primary School. The policy covers the use of still photography, video and any electronic equipment used to take images of children whilst in the care of our school. The policy sets out the expected protocols and requirements to ensure the safeguarding of children within our school is maintained. This policy adheres to the requirements of the Data Protection Act 1998, Copyright, Designs and Patent Act 1988, Human Rights legislation and the Equality Act 210. The Governing Board will ensure that the policy is reviewed and revised to take account of new and emerging guidance where appropriate.

Please delete as appropriate:

- This is a revised policy