	The Brakenhale School *High Expectations and Challenge for All*	GREENSHAW LEARNING TRUST

Policy Title
E-Safety Policy & Guidance

Date ratified by the FGB	June 2015	**For review by:**	June 2018
Staff Responsible	E-Safety Lead (SLT Member in charge of ICT Systems)	**Implemented by**	All Staff

Links to other policies	Curriculum policy; Safeguarding and Children Protection Policy; Student Behaviour Policy; Anti-Bullying Policy; Freedom of Information and Data Protection Guidance on the use of Mobile Electronic Devices

Rationale

This policy provides guidance on effective approaches to e-safety for the students and staff of The Brakenhale School.
It covers:

- **Policies and guidance** to support the e-safety of students, staff and adults volunteering with the school
- The **responses** necessary when a risk is discovered
- **Awareness-raising** for students, their parents/carers and staff and volunteers so that they are able to keep themselves, as well as those in their care, as safe as possible when using the internet and other electronic communication technologies

It is essential that existing policies are applied to the digital environment and regularly reviewed against this e-safety guidance and updated as necessary.

This guidance can be used as a stand-alone document or it can be used to inform existing policies. It should also be read in conjunction with the following:

Bracknell Forest Community Safety Partnership's (CSP's) e-safety Strategy and Action Plan, available on line at: (http://www.bracknell-forest.gov.uk/esafety)
The Berkshire Local Safeguarding Children Board Child Protection Procedures, available on line at: (http://proceduresonline.com/berks/)
The Berkshire Safeguarding Adults Policy and Procedures (January 2015), available on line at: (http://berksadultsg.proceduresonline.com/index.htm).

The Policy

The Governing Body and Headteacher work to ensure that students, staff and volunteers are able to use The Internet and related communications technologies appropriately and safely and this is addressed as part of the wider duty of care to which all who work in schools are bound. This school e-safety policy is written to ensure safe and appropriate use.

Students at The Brakenhale School will be taught the knowledge and skills to use technology safely and to understand their responsibilities for protecting themselves and others from harm.

Appropriate action will be taken by the school should disrespectful and/or improper use of technology (including The Internet and any form of social media) occur and if the guidance provided in this document is not followed.

Within the curriculum

a) Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.
- Internet use is an essential part of the curriculum and a necessary learning tool for staff and students.

b) Internet use will enhance and extend learning

- Staff will be made aware of and students will be educated in the safe use of the Internet.
- Clear boundaries will be set and discussed with staff and students, for the appropriate use of the Internet and digital communications.

c) Students will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Students will be made aware of how they can report abuse and who they should report abuse to.
- Students will be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Students will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

d) Managing monitoring and filtering

- The school will work in partnership with Greenshaw Learning Trust to ensure that systems to protect students are continuously reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Leads or the Systems Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- All Internet activity is logged by the school's Internet provider. These logs may be monitored by authorised Brakenhale School staff.

e) Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti- virus software before being used.
- No students or staff should interfere with any anti-virus software installed on school ICT equipment.
- Machines not routinely connected to the school network must be updated regularly with virus updates by ICT Support.
- If a virus is suspected on any school ICT equipment, use of the equipment should be stopped immediately and the Systems Manager contacted immediately. The Systems Manager will advise the actions to be taken and be responsible for advising others that need to know.

f) Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. The school will monitor this and continue to research solutions to this potential issue.
- Mobile phones will not be used during lessons or formal school time unless authorized by a member of staff (see the school's most recent Guidance on the use of Mobile Electronic Devices policy).
- The sending of abusive or inappropriate messages is forbidden.

g) Protecting personal data

- Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998.
- Staff will so far as possible not leave any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked with a pin code and kept out of sight.
- It is the responsibility of individual staff to 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 devices (multi-function print, fax, scan and copier) are used.

Managing Internet Access

h) Information system security

- School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

i) E-mail

- Students and staff should only use approved school e-mail accounts at firstlettersurname.brakenhale.co.uk
- Students and Staff must be made aware of how they can report abuse and who they should report abuse to.
- Students and Staff must report if they receive an offensive or inappropriate e-mail.
- In e-mail communications, students and staff must not reveal their personal details or those of others, or arrange to meet anyone without specific permission from the relevant line manager.

j) Published content and the school website

- Staff or student private and personal contact information will not be published. The contact details of staff provided will be the person's official school e-mail address.

k) Publishing students' images and work

- Written permission, using the approved permission forms, from parents or carers will be obtained before photographs of students are published on the school Website/ VLE, social media and any other publications.

l) Social Media and personal publishing

- The school will educate people in the safe use of social media, including Facebook and Twitter.
- Staff using social media for school purposes must use the agreed platforms used by the school.
- Staff wanting to set up departmental sites or pages can do so in consultation with the E-Learning Manager who will be able to monitor content posted.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately

and solely to the school's network and deleted from the staff device.

- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Headteacher.

m) Arrangements for Monitoring & Evaluation

The success of this policy and e-safety provision is maintained by the Systems Manager and the E-Safety Leads in the school - The Designated Child Protection Co-ordinator and the SLT Line Manager for ICT. It will be monitored and evaluated through:

- SIMS behavioural reports
- IT filtering systems
- The tracking of security breaches/data loss

n) CCTV

- The school uses CCTV for security and safety. Access to this is restricted and covered by the Data Protection Act. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school.

Policy Decisions

a) Authorising Internet access

- All staff, governors and visitors must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource, including any laptop issued for professional use.
- The school will maintain a current record of all staff, governors, visitors and students who are granted access to school ICT systems.
- Secondary age students must apply for Internet access individually by agreeing to comply with the school's ICT Acceptable Usage policy by signing relevant pages in the student diary.

b) Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Bracknell Forest Council can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- The school will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

c) Handling e-safety complaints

- Complaints of Internet misuse will be reported to the Senior Information Risk Owner and action in-line with the Bracknell Forest Safeguarding Children Board e-Safety policy will be taken.
- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the Designated Officer within one working day in accordance with Bracknell Forest Council Safeguarding Board policies.
- Any complaint about staff misuse must be referred to the head teacher and if the misuse is by the head teacher it must be referred to the chair of governors in line with Bracknell Forest Council Safeguarding Board Child Protection procedures.
- Students, parents and staff will be informed of the complaints procedure.

Communicating e-Safety

a) Introducing the e-safety policy to students

- E-Safety rules will be posted in all rooms where computers are used.
- All system users will be informed that network and Internet use will be monitored.
- A programme of e-Safety training and awareness raising will be put in place in-line with the Bracknell Forest Council Safeguarding Children Board's e-Safety Strategy.

b) E-Safety in the Curriculum

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

- The school provides opportunities within a range of curriculum areas to teach about e-safety.
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum.
- Students are aware of the relevant legislation when using the Internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.

c) Staff and the e-Safety policy

- All staff will be given access to the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user, including staff laptops.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

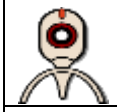
d) Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will hold parent/carer information sessions on e-safety.

APPENDICES

Appendix A

e-safety Rules

	Ask permission before using the internet
	Tell a trusted adult if you see anything that makes you feel uncomfortable
	Immediately close any webpage that you are uncomfortable with
	Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details
	Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos
	Only contact people that you have actually met in the real world
	Never arrange to meet someone that you have only met on the internet
	Only use a webcam with people you know
	Think very carefully about any pictures that you post online
	Never be mean or nasty to anyone on the internet or when using a mobile phone. If you know of someone being mean to another person, tell a trusted adult
	Only open e-mails from people that you know
	Avoid using websites that you wouldn't tell anyone about and use a student friendly search engine such as http://www.askforkids.com

Appendix B

Internet Safety Tips and Tricks

It is important for carers to remind any vulnerable person who uses the internet or other communication technology of the following:

- Always explore the privacy settings of your social networking site to protect your privacy and to protect yourself from strangers (for a range of online tutorials, go to http://www.kidsmart.org.uk/skills-school/)

- Facebook users can download a CEOP application to their Facebook page at http://apps.facebook.com/clickceop which enables quick access to help at a touch of a button

- Get friends and family to have a look at your social networking site to check that you aren't giving out too much personal information or posting inappropriate photos/films. They might see something you've missed
  - Keep your passwords to yourself
  - Respect yourself and others online

- If you are unlucky enough to have a bad experience, online report it to the service provider and tell a trusted person. You can also report to: CEOP REPORT ceop.police.uk

  or phone 101 (police non-emergency number)

- Cyberbullying is never acceptable. If you or someone you know is targeted by bullies online, tell them to:
  - report the bully to the website/service operator
  - keep evidence of the bullying behaviour
  - resist the temptation to reply to nasty messages
  - tell a trusted person

For more advice and tips, go to: http://www.bracknell- forest.gov.uk/esafety

Appendix C

Be safe when using the Internet

Ask someone you trust to make sure you are safe on the internet and Facebook
(find out more at http://www.kidsmart.org.uk/skills-school/).

Never tell anyone anything about you on the internet.

Never show them pictures. Tell someone you trust what you talked about on the internet.

Never tell anyone your passwords.

Be nice to others online.

On Facebook, click on http://apps.facebook.com/clickceop.
You will get a button.
Click on it if someone does something bad to you on Facebook.

If someone is nasty to you on the internet, tell someone who looks after you.
Phone 101 to tell the police, or www.ceop.police.uk

Never let people say nasty things to you on the internet. If they are:

- Tell the website
- Do not delete the nasty things they said
- Do not speak to them anymore
- Do not say nasty things to them
- Tell someone you trust

For more tips, go to:
http://www.bracknell-forest.gov.uk/esafety

Appendix D

The Brakenhale School

High Expectations and Challenge for All

Acceptable Use Policy for Staff and Volunteers

This covers use of digital technologies in the school i.e. e-mail, internet, intranet and network resources, learning platforms, software, mobile technologies, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed reasonable by the manager.
- I will only use approved e-mail and data system(s) for any school business (personal e- mail accounts are not secure systems).
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches to the manager.
- I will not allow unauthorised individuals to access e-mail / internet / intranet / networks or systems.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual other than myself.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed.
- I will follow the DSCF 2009 'Guidance for Safer Working Practice for Adults who work with Children and Young People' (http://www.timeplan.com/uploads/documents/Downloads/Safer-Working-Practices.pdf)
- I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I will not allow children and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I understand that all internet and network usage can be logged and this information could be made available to my manager on request.
- I will not connect a computer, laptop or other device to the network/internet that has not been approved by the school and meets its minimum security specification.
- I will not use personal digital cameras or camera phones for transferring images of children and young people or staff without permission.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that the Data Protection Act requires that any information seen by me with regard to staff or children and young people, held within any school system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will at all times behave responsibly and professionally in the digital world and will not publish any work-related content on the internet.

- I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.
- I understand that failure to comply with this Acceptable Use Policy (AUP) could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand The Brakenhale School's most recent Acceptable Use Policy (AUP).

I agree to abide by the school's most recent Acceptable Use Policy:

Signature…… Date……

Full Name …… (please print)

Agency (if applicable) e.g. supply teacher, BFC EWO, TVP Liaison Officer, Connexions or outsourced staff (kitchen, cleaners, security or ICT)

Job title:……Date……

Organisation:……

E-Safety Lead Authorised Signature

I approve this user to be set-up:

Signature…… Date……

Full Name …… (please print)

Appendix E

Inappropriate and Illegal Online Acts

Children, young people, vulnerable adults as well as organisation staff and volunteers who work with them must be aware of what is considered to be criminal when using the internet and electronic communication technologies. This should be reflected in the AUPs and education programmes delivered on an ongoing basis. While the list below is not exhaustive, it is hoped to provide some guidance in assessing the seriousness of incidents as well as determining appropriate actions.

It is noted that all incident types below are considered criminal in nature but would be subject a full investigation in order to determine whether a crime has been committed or not.

- Copyright infringement through copying diagrams, texts and photos without acknowledging the source
- Misuse of logins (using someone else's login)
- Distributing, printing or viewing information on the following:
    - Soft-core pornography
    - Hate material
    - Drugs
    - Weapons
    - Violence
    - Racism
- Distributing viruses
- Hacking sites
- Gambling
- Accessing age restricted material
- Bullying of anyone
- Viewing, production, distribution and possession of indecent images of children[1]
- Grooming and harassment of a child or young person
- Viewing, production, distribution and possession of extreme pornographic images
- Buying or selling stolen goods
- Inciting religious hatred and acts of terrorism
- Downloading multimedia (music and films) that has copyright attached. (Although this is illegal most police forces would treat this as a lower priority than the cases above)[2]

[1] Where the victim is under the age of 18 (recently changed from 16 years old by Section 1 of the Protection of Children Act 1988, as amended by the Criminal Justice and Public Order Act 1994 and Schedule 6 of the Sexual Offences Act 2003) and where the offender has attained the age of 10 (criminal age of responsibility). It is noted that the viewing of information of this nature may, in some circumstances, be appropriate i.e. research on hate crime, drugs etc.

[2] Compiled in consultation with Thames Valley Police and SEGfL

Appendix F

Facebook Guidance for Schools (Cyberbullying/Inappropriate Behaviour)

1. If you know the identity of the perpetrator, contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed, often works.
2. Failing that, having kept a copy of the page or message in question, delete the content.
3. For messages, the 'delete and report / block user facilities' are found in the 'Actions' dropdown on the page on which the message appears.
4. For whole pages, the 'unfriend and report / block user facilities' are at the bottom of the left hand column. Always try to cite which of the Facebook Terms and Conditions have been violated (see note 10 for the most likely ones) at http://www.facebook.com/terms.php or Community Standards at http://www.facebook.com/communitystandards/. Note that Facebook are more alert to US law than UK. The process should be anonymous.
5. If the page is by someone under 13 click on http://www.facebook.com/help/contact.php?show_form=underage (Facebook say they will delete any such page).
6. To remove a post from a profile, hover over it and on the right there will be a cross to delete it.
7. Does the incident trigger the need to inform the police or child protection agencies?
8. To report abuse or harassment, email abuse@facebook.com (Facebook will acknowledge receipt of you email and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint).
9. If all else fails, support the victim, if they wish, to click the 'Click CEOP' button http://www.thinkuknow.co.uk/

10. If the victim is determined to continue using Facebook, they might want to delete their account and start again under a different name. Deletion can be done here https://ssl.facebook.com/help/contact.php?show_form=delete_account. They should be made aware of the privacy issues that might have given rise to their problem in the first place:

    - You will not bully, intimidate, or harass any user (1.3.6)
    - You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission (4.1)
    - You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law (5.1)

NOTE: An effective education programme can help to reduce the number of times that this sort of incident arises, over the medium term. Such a programme should help young people to match their online behaviour with their offline behaviour by helping them to develop understanding, skills and behaviours in these sorts of areas:

- possible consequences
- understanding the effects of bullying on others
- understanding how technology can magnify impact
- understanding how comments or other actions can be perceived differently by the originator and the target

Further Guidance

CEOP (Child Exploitation and Online Protection Centre)
http://www.ceop.gov.uk

The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. That means that they are part of UK policing and very much about tracking and bringing offenders to account either directly or in partnership with local and international forces.

Think U Know
http://www.thinkuknow.co.uk

Think U Know is CEOP's support, guidance and resource site for children, young people, parents, carers and adults who work with children and young people.

UK Safer Internet Centre
http://www.saferinternet.org.uk/

This website provides the latest advice on how to use the internet and new technologies safely and responsibly. Also find a range of practical resources, news and events focussing on the safe and responsible use of the internet and new technologies.

Childnet
http://www.childnet-int.org

Childnet is a non-profit organisation working with others to "help make the Internet a great and safe place for children". The website gives news and background to Childnet's work and serves as a portal to Childnet's award-winning projects.

Bracknell Forest e-safety webpage
http://bracknell-forest.gov.uk/esafety

These pages define e-safety, describe the possible risks and also detail what Bracknell Forest is doing to safeguard vulnerable users of the internet and other digital technologies in the Borough. It also includes useful resources such as leaflets, videos and guidance which can be downloaded and used within organisations/settings to raise awareness of the risks and how to be safe.

Teach Today
http://www.teachtoday.eu/en/Teacher-advice/Cyberbullying.aspx

Teachtoday provides information and advice for teachers, head teachers, governors and other members of the school workforce about the positive, responsible and safe use of new technologies. The above link provides advice and guidance on cyberbullying towards teaching staff.

NASUW T: The Teachers' Union
http://www.nasuwt.org.uk/Whatsnew/Campaigns/StopCyberbullying/index.htm

The NASUWT is the largest teachers' union in the UK. The NASUWT is the only TUC-affiliated teachers' union to represent teachers in England, Northern Ireland, Scotland and Wales. NASUWT organises in all sectors from early years to further education and represents teachers in all roles including heads and deputies. NASUWT is politically independent and is deeply committed to working to influence the education policy of the Government and employers. The above link provides guidance and support on the subject of cyberbullying towards teaching staff.

Appendix G

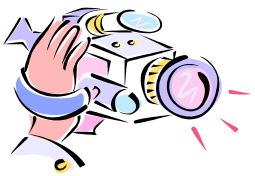
The Brakenhale School
E-Safety Form- Expectations of Parents

High Expectations and Challenge for All

e-safety form: Expectations of Parents

Internet and ICT: As the parent/carer or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to: ○ the Internet at school ○ the school's chosen email system ○ the school's online managed learning environment ○ ICT facilities and equipment at the school.	✓
I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.	✓
I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.	✓
Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.	✓
I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.	✓
I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.	✓
I will not take and then share online, photographs of other children (or staff) at school events without permission.	✓
Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.	✓
I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.	✓
I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.	✓

The use of digital images and video



To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

- **If the pupil is named, we avoid using their photograph.**
- **If their photograph is used, we avoid naming the pupil.**
- Where showcasing examples of pupil work we only use their first names, rather than their full names.
- If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
- Only images of pupils in suitable dress are used.
- Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made, as part of the learning record, and then sharing with their parent / carer.
- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays or PowerPoint© presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
- CCTV footage to identify students.
- In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

This school asks its whole community to promote the 3 common approaches to online behaviour:

Common courtesy **Common decency** **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic, biphobic, transphobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, pupil or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

Child's Name: _____

Parent's signature: _____

Appendix J

The Brakenhale School

High Expectations and Challenge for All

STUDENT ACCEPTABLE USE POLICY

Technology is an essential element in the 21st century. ICT (including the school network, information portals, internet, learning platforms, email and mobile technologies) has become an important part of learning in our school. We expect all students to be safe and responsible and to stay safe when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT. Please read through the school policy carefully.

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ learning platform with my own user name and password.
- I will follow the school's ICT security system, I will not reveal my passwords to anyone and I will change my passwords regularly.
- I will only use my school email address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring them into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet, school network and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

The school has a comprehensive **e-Safety Policy** which can be found on the Policy page of the school website at http://brakenhale.co.uk/policies/

Please sign to say that you understand and agree to follow the Acceptable Use Policy

Student Signature: _____ Date: _____

Parent Signature: _____ Date: _____

Tutor Signature: _____ Date: _____