BURLINGTON JUNIOR SCHOOL

Online safety Policy

Written By	**Senior Leadership Team**	
Frequency of Review	**1 year**	
Date reviewed and approved by Governing Body	**March 2018**	
Date of next review	**March 2019**	
Display on Website	✓	
Purpose	**Outlines the safeguards and precautions in place in school to ensure safe internet access for our children at all times.**	
Consultation	**Governors**	✓
	Parents	✓
	Pupils	✓
	Staff	✓
Links with other policies	**Child Protection** **Safeguarding**	

Internet Access and Online safety Policy. March 2018

We believe that the internet can provide our children with a wonderful learning resource; however we are also aware that we must take every precaution to ensure safe internet access for our children at all times.
This is done through the following measures:

- All computers in the suite are connected to the internet and children are taught to access this as appropriate.
- Access will be monitored using Securus online safety software for device owned by the school and connected to the secure WiFi network.
- Children's identity is protected with provided secret passwords.
- Children will be taught the importance of password privacy.
- When instances arise of children's passwords becoming known by other children the passwords will be changed.
- Staff will select sites which will support the learning outcomes planned for children.
- Internet access will be planned to enrich and extend learning activities.
- Children are supervised when using the internet and emailing but are expected to share immediately with the teacher any material that they think is inappropriate.
- Children will be given clear guidance for internet use, and only ever be allowed to access approved educational sites selected by staff.
- The children will never be given access to unsupervised open chat rooms.
- Children will be taught to send and receive emails through our intranet (from children and teachers within the school).
- Children must sign an Acceptable use policy each year which will be held by the school.
- Parents must sign a separate Acceptable use policy each year which will be held by the school.
- Children will be taught to log off after computer use.
- The school will work in partnership with the Achieving For Children, DFES and our internet service provider to ensure systems to protect pupils are reviewed and improved.
- The school has the view of not over filtering websites so that children have a safe environment to learn how to make the right choices if they see something they are not happy with e.g. Youtube is currently allowed for pupils to access.

The school recognises its responsibility to educate our children to protect themselves outside of school. To this end:

- Children will be made aware of issues surrounding uncertainty of online identities and revealing personal data.
- Children will be made aware of the PEGI age restrictions applied to some games.
- These issues will be covered in every year group and assemblies.
- online safety will be discussed in all classes in September and children reminded of this in December, Safety Internet Day (February) and Summer term.
- Meetings and/or workshops to raise parental awareness of online safety will be arranged at least twice a year.
- Staff will discuss suitable time to spend online as to promote positive mental health.

The school uses a security system (Securus) which takes a screen shot should inappropriate language or images be used. However, this system does not cover children using electronic devices at home.
The following information is taken from the NSPCC website. These issues will be discussed with children in classes at an age appropriate level. Should an issue arise which possibly highlights online safety concerns then teachers will either contact the whole class or individual parents.

Cyberbullying

Cyberbullying is a growing problem and includes:

- sending threatening or disturbing text messages.
- homophobia, racism or sexism.
- making silent, hoax or abusive calls.

- creating and sharing embarrassing images or videos.
- trolling; the sending of menacing or upsetting messages on social networks, chat rooms or online games.
- excluding children from online games, activities or friendship groups.
- setting up hate sites or groups about a particular child.
- encouraging young people to self-harm.
- voting for someone in an abusive poll.
- hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

Sharing images online (Sexting)

This is just as relevant in the upper primary years as with secondary school years. Children are having earlier experiences with using social media sites and new Apps (sometimes with parental permission, sometimes secretly) even though the age restrictions on these are quite clear.
In Burlington we aim to help children understand that sending images or 'sexting' (photographs, videos and live streaming) of themselves can be dangerous. Students are also made aware of the rise of incidents involving sextortion.

1. The victim has no control over how the image is used or passed on.
2. Sending images is often seen as flirting by children and young people who feel that it is part of normal life.
3. Most young children are reluctant to talk to adults about it because they are afraid of being judged or having their phones/ i pads/ tablets taken away.
4. Parents and children need to be aware of the risks of sending images that could be misused immediately or in the future.
5. Parents and children also need to be aware of the growing problem of blackmailing. In this case children are often invited to send further images rather than risk having pictures posted publicly or sent to family members.

Parents also need to be are that 'sharenting' can be harmful to children's self-esteem. This is where parents put images and pictures of children online which are later found to embarrass them as they get older.

Peter Cowley (AfC) is regularly invited into school to update staff (Autumn 2017) and pupils and parents (Autumn 2017) on all issues concerned with online safety.

Appendices.
Appendix 1 Burlington Junior School online safety form for parents
Appendix 2 Burlington Junior School online safety form for pupils
Appendix 3 Burlington online safety expectations
Appendix 4 The use of digital imagery and video
Appendix 5 Videos games and keeping children safe for parents
Appendix 6 Letter to parents regarding gaming safety
Appendix 7 Letter to parents regarding knowledge of a Facebook account

Appendix 1

Burlington Junior School Acceptable Use agreement for parents

Burlington Junior School regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies, which can be found on our school website. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning. We expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.

Your child will be asked to read and sign an Acceptable Use Policy tailored to their age. Please read this carefully – it is available on our school website.

Parents Acceptable Use Agreement

Internet and IT: As the parent 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**
- **blogging platforms (J2E)**
- **IT 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 all internet and devices used in school are subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used in the same manner as when in school.

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.

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. The impact of social media use is often felt in schools, and this is why we expect certain behaviours from pupils when using social media at all times.

I will not take and then share online, photographs, videos etc. about other children (or staff) at school events, without the school's permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I understand that my son/daughter has agreed in the pupil acceptable-use policy not to search for or share any material that could be considered offensive, harmful or illegal. This might include bullying or extremist/hate/discriminatory content.

I will support the school by promoting safe and responsible use of the internet, online services and digital technology at home. I will inform the school if I have any concerns.

Name(s) of pupil/student: _____Class _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

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

Burlington Junior School rules for any external use of digital images are:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' 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 in a lesson.
- 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. in our school prospectus or on our school website. On rare occasions, 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 they won a national competition and wanted to be named in local or government literature.

Appendix 2

Burlington Junior School Acceptable Use agreement for pupils

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** **– I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.**
- ***I am a secure online learner*** **– I keep my passwords to myself and reset them if anyone finds them out.**
- ***I am careful online*** **– I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.**
- ***I am private online*** **– I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.**
- ***I keep my body to myself online*** **– I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.**
- ***I say no online if I need to*** **– if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.**
- ***I am a rule-follower online*** **– I know that some websites and social networks have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to.**
- ***I am considerate online*** **– I do not join in with bullying or sharing inappropriate material.**
- ***I am respectful online*** **– I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.**
- ***I am part of a community*** **– I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.**
- ***I am responsible online*** **– I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.**
- ***I don't do public live streams on my own*** **– and only go on a video chat if my trusted adult knows I am doing it and who with.**
- ***I communicate and collaborate online*** **– with people I know and have met in real life or that a trusted adult knows about.**
- ***I am SMART online*** **– I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.**
- ***I am a creative digital learner online*** **– I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.**
- ***I am a researcher online*** **– I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.**

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Name: _____

Signed: _____ **Date:** _____

APPENDIX 3

Burlington online safety Expectations for our School Community

The use of social networking and on-line media

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

(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
This school asks its whole community to promote the 3 commons approach to online behaviour:
o Common courtesy
o Common decency
o Common sense

Common Courtesy
o 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.

Common Decency
o We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is cyber bullying and may be harassment or libel.
o 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.

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

In the event that any member of staff, student or parent/carer is found to be posting libellous or defamatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

Appendix 4
The use of digital imagery and video

We will only use children's first names with images or videos.
Only images of pupils in suitable dress are used.
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 by a child, as part of the learning record, and then sharing with their parent / guardian.
• Your child's image being used for presentation purposes around the school on paper or electronically.
• 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.

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.

Appendix 5
Video Games and keeping your child safe : parents

Burlington Junior School is committed to keeping our children safe and to promoting the safe, responsible use of the technologies.

1) Ratings denote the content and appropriateness of games
Since 2003 games have been age rated under the Pan-European Game Information (PEGI) system which operates in the UK and over 30 other countries of Europe, in addition, where a game showed realistic scenes of gross violence or sexual activity the game had to be legally classified and received one or other of the BBFC classification certificates given for videos/DVDs

The PEGI system has been effectively incorporated into UK law and video games will be age rated at one or other of the following age levels; which you will find on video game sleeves. Ratings do not denote the difficulty or the enjoyment level of a game, but that that it contains content suitable for a certain age group and above

The PEGI age ratings will enable parents and carers to make an informed choice when buying a game for their children.

It is important to note that the age ratings 12, 16 and 18 age ratings are mandatory and that it is **illegal** for a retailer to supply any game with any of these ratings to anyone below the specified age. The age ratings 3 and 7 are advisory only.

An 18 Rated game is applied when the level of violence reaches a stage where it becomes gross violence and/or includes elements of specific types of violence.
In general terms it is where the level of violence is so visually strong that it would make the reasonable viewer react with a sense of revulsion.

This rating is also applied where the level of sexual activity is explicit which may mean that genitals are visible. Any game that glamorises the use of real life drugs will also probably fall into this category.

2) Content Indicators

In addition to age ratings, video games will include indicators of the type of content and activities that the game includes in it.
The descriptors are fairly self-explanatory but should be read in conjunction with the age rating given for a video game.

A violence descriptor with an 18 rated game will indicate a more extreme level of violence than a violence descriptor with a 12 rated game. Similarly a sex/nudity descriptor with a 12 rated game will probably indicate sexual innuendo but a sex/nudity descriptor with an 18 rated game will indicate sexual content of a more explicit nature.

3) Parental responsibility

We feel it is important to point out to parents the risks of underage use of such video games, so **you** can make an *informed* decision as to whether to allow your child to be subjected to such images and content.

The PEGI ratings system helps you make informed decisions about which video games to choose for your family
A PEGI rating gives the suggested minimum age that you must be to play a game due to the suitability of the content
As parents you can take direct control of what games your children play at home, how they play them and for how long through parental controls on video game systems such as the Xbox or Playstation
Choosing and playing video games as a family is the best way to understand and enjoy them together
The stories, worlds and characters in video games offer playful ways to engage with a wide range of subjects and fuels creativity, interests and imagination
The recently re-launched askaboutgames.com website provides further information about video games ratings and offers real family stories and suggestions on how video games can be a creative and collaborative experience for all the family
We also recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online www.thinkuknow.co.uk

Appendix 6

Letter to parents regarding gaming safety

Dear Parent/Carer,

Video Games and keeping your child safe:

Child's name: _____ Class: _____

It has been brought to our attention that your child has been playing console games such as GAME NAME, even though the certification for this game is 18 based on International PEGI ratings.

At Burlington Junior School we are committed to keeping our children safe and to promoting the safe, responsible use of the technologies. As such, we feel it is our responsibility to raise this particular issue as a concern.

It is important to note that the age ratings 12, 16 and 18 age ratings are mandatory and that it is illegal for a retailer to supply any game with any of these ratings to anyone below the specified age. The age ratings 3 and 7 are advisory only.

An 18 Rated game is applied when the level of violence is so visually strong that it would make the reasonable viewer react with a sense of revulsion; where the level of sexual activity is explicit which may mean that genitals are visible or any game that glamorises the use of real life drugs will also probably fall into this category.

In addition to age ratings, video games will include indicators of the type of content and activities that the game includes in it.

We feel it is important to point out to parents the risks of underage use of such video games, so you can make an *informed* decision as to whether to allow your child to be subjected to such images and content.

If you feel that you, or your child, needs further support in keeping your child safe on the internet, please make an appointment to see NAME (Head of Key Stage). Because of our duty to all the children in our school, we will take action (which may involve the police) if a problem comes to our attention that involves the safety or wellbeing of any of our pupils.

With thanks for your continued support,

Headteacher

Appendix 7
Letter to parents regarding knowledge of a Facebook account

Dear Parent/Carer,

Facebook and keeping your child safe

It has come to our attention that _____ has a Facebook profile even though the permitted minimum age to use the site is 13, according to the sites terms and conditions.

Burlington Junior School is committed to promoting the safe and responsible use of the Internet and as such we feel it is our responsibility to raise this particular issue as a concern. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind and this is specifically over 13 years old. Possible risks for children under 13 using the site may include:

- Facebook use "age targeted" advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered
- Children may accept friend requests from people they don't know in real life which could increase the risk of inappropriate contact or behaviour
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and options
- Facebook could be exploited by bullies and for other inappropriate contact
- Facebook cannot and does not verify its members therefore it is important to remember that if your child can lie about who they are online, so can anyone else!

We feel it important to point out to parents the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friends, siblings or even parents. We will take action (such as reporting under aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children.

Should you decide to allow your child to have a Facebook profile we strongly advise you:

- Check their profile is set to private and that only friends can see information that is posted
- Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark on their profile to CEOP and the Report Abuse button which has been known to deter offenders
- Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents
- Set up your own profile so you understand how the site works and ask them to have you as a friend on their profile so you know what they are posting online
- Make sure your child understands the following rules:
  - Always keep your profile private
  - Never accept friends you don't know in real life
  - Never post anything which could reveal your identity
  - Never post anything you wouldn't want your parents to see
  - Never agree to meet somebody you only know online without telling a trusted adult
  - Always tell someone if you feel threatened or someone upsets you

We'd recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online www.thinkuknow.co.uk

If you would like any further information please don't hesitate to contact us.

Class Teacher