BROWNHILLS SCHOOL

E-Safety Policy

Review Date: January 2019

E-Safety Designated Person:
Mrs P. Tomlinson

This policy **MUST** be read in conjunction with Brownhills School Child Safeguarding Policy, Behaviour Policy, ICT Acceptable Use Policies and our Anti-bullying Policy

INTRODUCTION

What is e-safety?

Brownhills School believes that the use of information and communication technology in school brings great benefits. This policy aims to recognise e-safety issues and will help to ensure the appropriate, effective and safer use of electronic communications for all pupils and staff.

We are aware that in today's society children, young people and adults interact with technologies such as; mobile devices (including phones, tablets, wearable technology e.g. smart watches), games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved can be greatly beneficial to all, but can also place children in danger.

This e-safety policy covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communication technologies, **both in and out of school.**

Aims

- To safeguard children, young people and staff.
- To be able to identify the risks associated with social networking.
- To identify roles and responsibilities and recognise that e-safety is part of the 'duty of care' which applies to everyone working with children.
- To educate and empower children so that they possess the necessary skills to make safe and responsible decisions and to feel confident to report any concerns they may have.
- To raise awareness of the importance of e-safety amongst all staff so they are able to educate and protect children in their care.
- To inform staff how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.
- To provide opportunities for parents/carers to develop their knowledge of e -safety.
- **To ensure awareness amongst all members of Brownhills School that 'online actions can have offline consequences'.**

ACCEPTABLE USE POLICIES (Students and Staff)

Important information

Breaches of an acceptable use policy can lead to civil, disciplinary and criminal action been taken against staff, pupils and members of the wider school community.

All pupils, students, trainees and staff will be expected to accept our ICT Acceptable Use Policies each time they log onto the school network either on or off site.

Parents/carers of pupils in Key Stage 3 and 4 will also be asked to read our home School agreement.

Further staff guidance for personal use and social networking will be discussed as part of staff induction and safe and acceptable professional behaviour is outlined in all of our network related policies (found in the staff shared area).
(Please also see ***Appendix A*** -
Staff Guidance for Participating in Social Networking)

Brownhills School will ensure that:

- The e-safety policy will be reviewed annually.
- A member of the Senior Leadership team has responsibility for e-safety in school.
- All members of the school community will be informed about the procedure for reporting e-safety concerns (such as breaches of filtering, Cyber-bullying, illegal content).
- The Designated Safeguarding Officer will be informed of any e-safety incidents involving Safeguarding concerns, which will then be acted on appropriately.
- The school will manage e-safety incidents in accordance with the school's behaviour and Anti-bullying policies where appropriate.
- The school will inform parents/carers of any incidents of concern as and when required.

- Where there is a cause for concern or fear that illegal activity has taken place or is taking place, then the school will contact the Children's Safeguarding Team for advice and/or escalate the concern to the Police.
- The Police will be contacted if a criminal offence is suspected.
- Any complaint about staff misuse must be directly reported to the Headteacher.
- We work in partnership with Parents/Carers and pupils to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and Safeguarding procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of **not** posting any content, comments, images or videos online **which cause harm, distress or offence to any other members of the school community**.

CYBER-BULLYING

Cyber-bullying can be defined as '*The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone*' DCSF 2007.

Many children, young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively and we have a duty to safeguard all pupils and staff.

When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone. This can be harmful, threatening and a great source of anxiety.

Where bullying outside school (such as online or via text message/voicemail) is reported to school, it will be investigated and acted on.

Brownhills School will ensure that:

- Cyber-bullying (along with all other forms of bullying) of any member of the school will NOT be tolerated. Full details are set out in the school's behaviour and anti-bullying policy.
- There are clear procedures in place to support anyone in the school community affected by Cyber-bullying.
- There are clear procedures in place to investigate incidents or allegations of Cyber-bullying (see Anti-Bullying Policy).

MOBILE DEVICE POLICY

Please refer to the Mobile Phone policy which is detailed in the student planners and is available on the staff shared area.

- Mobile Phones, or any other mobile devices with integrated cameras, could lead to Safeguarding/Child Protection, bullying and data protection issues with regard to inappropriate capture or distribution of images of pupils or staff.
- Mobile phone use can render pupils or staff subject to Cyber-bullying.
- Internet access on mobile devices using cellular data cannot be filtered by the school.
- They can undermine classroom discipline.

ROLES AND RESPONSIBILITIES

Pupils and Staff MUST:

- Immediately report to a **designated member of staff** if they receive offensive or abusive emails, text messages or posts on social networking sites.
- Immediately report to a **designated member of staff** if they have information that another member of the school community has experienced any of the above.
- **Not** reveal personal details of themselves or others which may identify them and/ or their location.
- Set passwords to their accounts in and out of school.
- Deny access to unknown individuals and block unwanted communications on social network sites.
- **Not** publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

COMMUNICATING E-SAFETY

- E-safety information leaflet for pupils, parents and carers is available on the school website
- Providing ‘cyber-bullying’ government guidance for parents on the school website.
- An e-safety module will be delivered through Focus Days, covering both safe school and home use.

- The e-safety policy will be formally provided to, and discussed with, all members of staff and displayed on our school website.
- To protect all pupils and staff, the school will implement acceptable use policies.
- Parents attention will be drawn to the school e-safety policy, e-safety leaflet and in newsletters and on the school website.

- A partnership approach to e-safety at home and at school with parents will be encouraged by offering parental e-safety sessions in partnership with the relevant external agencies.
- Subject staff are encouraged to discuss / advise / take the opportunity to give e-safety reminders when using ICT in lessons.

E-safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Useful e-safety programmes include:

Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet.com Kidsmart: www.kidsmart.org.uk
Safe: www.safesocialnetworking.org Childline: www.childline.org.uk

APPENDIX A

Staff Guidance for Participating in Social Networking

Whilst the usefulness of social networks (including, but not exclusive to, Facebook, Twitter, MySpace, YouTube, etc.) is not disputed, Brownhills School staff choosing to use them must do all they can to protect their reputations and the reputation of the school.

As stated in Teachers' Standards (DFE, 2012) "A teacher is expected to demonstrate consistently high standards of personal and professional conduct. [Teachers must] uphold public trust in the profession and maintain high standards of ethics and behaviour, within and **outside school**".

Protect yourself

To ensure that all staff and trainee staff protect their reputations and their privacy you must:

- Not befriend pupils on social networking sites.
- Not access social network sites in school time.
- Not post information or personal views about Brownhills School, its staff, pupils or parents.
- Think carefully how you present yourself when posting images, joining a group or 'liking' pages as these choices say something about you.
- Choose your friends carefully, not accepting friend requests from pupils or parents.
- Control who can see your information (for example, setting 'friends only' on Facebook and 'protecting my tweets' on Twitter).
- Be careful about comments you post on friends' walls because, if their profiles are not set to private, your comments will be visible to everyone.
- 'Un-tag' yourself from any inappropriate content posted by others, or ask the person who has posted the content to remove it.
- Keep passwords secret.
- Report any incident to the appropriate member of staff in a timely manner.
- Do not leave a computer or any other device logged in when you are away from your desk unless you have 'locked' it.
- Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure that they are kept up to date.
- Use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites, for example Dropbox and YouTube.

Remember that anything you post online is potentially public and permanent.

General Rule

Social networks and their associated terminology ('wall', 'tag', etc) are constantly changing and situations may arise which this guidance does not cover. Therefore, a general rule to follow is to avoid compromising your professional position by always presenting yourself online to colleagues, pupils, parents and members of the community in the same way you would present yourself in person.

APPENDIX B

Getting offensive content taken down

If online content is offensive or inappropriate, and the person or people responsible are known, you need to ensure that they understand why the material is unacceptable or offensive and request they remove it.

Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material, the staff member should use the tools on the social networking site directly to make a report.

Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.

Before you contact a service provider, it is important to be clear about where the content is; for example by taking a screen shot of the material that includes the web address. If you are requesting that they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions. Where material is suspected of being illegal, you should contact the police directly.

Contact details for social networking sites

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools.

Site	Useful links
Ask.fm	Read Ask.fm's 'terms of service' Read Ask.fm's safety tips Reporting on Ask.fm: You do not need to be logged into the site (i.e. a user) to report. When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow, which allows you to report the post.
BBM	Read BBM rules and safety
Facebook	Read Facebook's rules Report to Facebook Facebook Safety Centre
Instagram	Read Instagram's rules Report to Instagram Instagram Safety Centre
Kik Messenger	Read Kik's rules Report to Kik Kik Help Centre
Snapchat	Read Snapchat rules Report to Snapchat Read Snapchat's safety tips for parents
Tumblr	Read Tumblr's rules Report to Tumblr by email If you email Tumblr, take a screen shot as evidence and attach it to your email
Twitter	Read Twitter's rules Report to Twitter
Vine	Read Vine's rules Contacting Vine and Reporting
YouTube	Read YouTube's rules Report to YouTube YouTube Safety Centre

APPENDIX C

e-safety

After your e-safety training these are YOUR top tips to keep us all safe when using the internet:

Don't add people that you don't know on social networking sites. You wouldn't talk to a stranger in the street, so why talk to them online?

Don't upload photographs of yourself that are inappropriate or give information away about yourself. You don't know how these images will be used by others!

Don't give away your personal details on the internet. You don't know who can access this information!

If you feel unsafe online, tell a parent, carer or teacher and click the report abuse button on the school website

CEOP REPORT
ceop.police.uk

www.barrbeaconschool.co.uk