E-Safety Policy

Publication date: September 2019
Review Date: September 2020

E-Safety Designated Lead:
Mrs U Simpson

Nominated Governor for e-Safety:
Mrs D Williams

This policy **MUST** be read in conjunction with Bloxwich Academy Child Safeguarding Policy,
Behaviour Policy and our Anti-bullying Policy

INTRODUCTION

1. What is e-safety?

1.1 Bloxwich Academy 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.

1.2 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.

1.3 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.**

2. 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 Bloxwich Academy that 'online actions can have offline consequences'.

3. ACCEPTABLE USE POLICIES (Pupils, Staff and 6th Form)

3.1 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 read our ICT Acceptable Use Policies and sign the appropriate consent documentation before an account is created.

- Parents/carers of pupils in Key Stage 3 and 4 will also be asked to read and sign an ICT acceptable use policy before their child's account is created. We would also ask that parents/carers discuss the ICT acceptable use agreement with their child, where appropriate.

- Further staff guidance for personal use and social networking will be discussed as part of staff induction and safe and acceptable professional behaviour will be outlined in the Staff Acceptable Use policy. (Please also see *Appendix A - Staff Guidance for Participating in*

Social Networking)

3.2 Bloxwich Academy will ensure that:

- A member of the Senior Leadership team has responsibility for e-safety in school.
- The school appoints a member of the Governing Body to take lead responsibility for e-safety..
- The designated e-safety lead will ensure they are fully briefed by completing appropriate 'keeping children safe on-line' courses
- All members of the school community will be informed about the procedure for reporting e-safety concerns (such as breaches of filtering, Cyberbullying, 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**.

4. CYBERBULLYING

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

4.2 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.

4.3 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.

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

\

4.5 Bloxwich Academy will ensure that:

- Cyberbullying (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 Cyberbullying.
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying (see Anti-Bullying Policy).

5. MOBILE DEVICE POLICY

5.1 Bloxwich Academy is a **NO MOBILE PHONE SITE** for Years 7-11. This also includes any other mobile or electronic devices such as tablets, phablets, smart watches and digital cameras. Members of the Sixth Form are permitted to carry mobile phones on their person however; no Sixth Form student is allowed to have their mobile phone on show in the presence of younger pupils. Our procedures, should a pupil bring their mobile phone into school, are clearly outlined in the Behaviour Policy.

- 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 Cyberbullying.
- Internet access on mobile devices using cellular data cannot be filtered by the school.
- They can undermine classroom discipline.

6. ROLES AND RESPONSIBILITIES

6.1 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.
- Follow Bloxwich Academy 'Top Tips for e-safety'.

7. COMMUNICATING E-SAFETY

- E-safety information leaflet for pupils, parents and carers is available on the school website **(Appendix C)**.
- Providing 'cyberbullying' government guidance for parents on the school website.
- E-safety posters with pupils' '*Top Tips'* for keeping safe when using the Internet will be displayed in a number of key locations in the school **(Appendix D)**.

- An e-safety training programme will be established across the school to raise the awareness and importance of safe and responsible Internet use amongst pupils.
- Regular training (CPD-Continuing Professional Development) will be provided for all staff to maintain a heightened awareness of technological and social issues related to e-safety.
- An e-safety module will be delivered through PSHE, 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 and a range of e-safety guidance posted on the school website from CEOP, NSPCC and Childnet
- 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 relevant external agencies.
- Parents/carers of pupils in Key stages 3 and 4 will be requested to sign an ICT acceptable use policy before their child has an account created in school.
- Subject staff are encouraged to discuss / advise / take the opportunity to give e-safety reminders when using ICT in lessons.

8. E-safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
NSPCC- Online safety www.nspcc.org.uk

Alternatively, click the following link **on our school website**:

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, Bloxwich Academy 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, 2011) "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 Bloxwich Academy, 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.
- 'Untag' 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

Site	Key information
Ask.fm	Read safety advice at http://safety.ask.fm/. Use the report button to alert ASKfm about any behaviour that breaks their terms. Use the block button to prevent someone from asking you any more questions
Moshi	Read the safety page—www.moshimonsters.com/parents Click the 'M' button or 'Report' button Or use the contact details on the bottom of every page
Facebook	Read the advice for parents and young people in the Safety Centre: www.facebook.com/safety also The Bullying Prevention Hub offers advice and resources
Instagram	Access advice from the Instagram's Help Centre. This includes details on blocking and reporting
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
WhatsApp	Read information on staying safe on WhatsApp FAQ page
YouTube	Read YouTube's rules Report to YouTube YouTube Safety Centre
Musical.ly	Musical.ly FAQ section gives advice on blocking, deleting and privacy settings. If you see inappropriate content you should click the button with three dots and then click 'report abuse'. Concerned parents can email info@musical.ly

APPENDIX C

Recommended rules for using the Internet at home

- Use a pupil friendly search engine and websites that are recommended by teaching staff
- Only speak to people you actually know online
- Know how to report abuse and block those unwanted users
- Only use a webcam with people you know
- Report concerns to the Child Exploitation & Online Protection Centre (CEOP)
- Be aware of comments that are being made and can be viewed by others
- Tell an adult that you trust IMMEDIATELY if you feel unsafe online

These are YOUR Top Tips to keep us all safe on the internet:

- Don't add people 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.

Recommended websites for further information:

CLICK CEOP Internet Safety — www.ceop.gov.uk

THINK U KNOW — www.thinkuknow.co.uk

How your child uses ICT

ICT is used in several lessons across our curriculum. Within lessons, pupils use a wide range of ICT including:

Word processing (Word) to write essays, news articles or letters

Databases (Access) to record information

Spreadsheets (Excel) to create tables, charts and graphs

Desktop Publishing (Publisher) to design posters, leaflets and cards

Multimedia (Powerpoint, Movie Maker or Final Cut) to present text, pictures and video

Drawing Programmes (Paint, Photoshop, CAD -Computer Aided Design) to create pictures and designs

Internet (Explorer) to research for project work

E-Mail (Outlook) to contact friends and email work to teachers

Video Conferencing (Skype) to share ideas or ask an expert

Digital Cameras to record classwork, coursework or research from a trip

Music Software (Sibelius & Garageband) to create compositions.

Our mobile phone policy

Bloxwich Academy is a NO MOBILE PHONE SITE

Our mobile phone policy has been written to ensure that all our pupils are safeguarded. You can view this policy on our school website.

It is vital that no pupil is allowed to have images of your child, in their possession, without your consent.

We would recommend that you know all passwords for your child's mobile phone and check this regularly.

e-Safety Information
For Pupils, Parents & Carers

Why is e-Safety important?

Young people today are increasingly using ICT in School and at home. At **Bloxwich Academy it is** within our duty of care for our pupils to ensure that we inform parents and carers of the following:

- How pupils use ICT in School
- How using ICT at home helps pupils to learn
- How the internet can be used safely at home
- Where to find out more information of how to be safe online

How you can help your child at home

ICT is not just about using a computer – it is the use of a mobile phone, digital camera, MP3 player or DVD player. Pupils can develop their ICT skills further at home by:

- Writing a letter or email to a relative
- Creating digital artwork or pictures
- Using the internet to research a project
- Using recommended websites to enhance learning e.g. BBC Bitesize

Benefits of using ICT at home

There are several advantages of having a computer and internet access at home. Some of these are:

- ICT can help pupils attainment
- Skills are developed for life
- Developing enjoyment of using ICT
- Able to access a wider range of learning materials
- Supports homework and revision
- Improves presentation of their work

Using the internet safely at home

Whilst we encourage the use of ICT for pupils to learn and access a wide range of material, it is within our duty of care to advise parents and carers to carefully monitor your child's use of the internet. Despite many internet service providers offering filtering systems and tools to help safeguard your child, it is still surprisingly easy to access inappropriate material including text, pictures and films.

We would recommend that your computer is in a family area if possible and not in a bedroom. Also please remember that many mobile phones, games consoles and electronic readers do allow access to the internet.

Bloxwich Academy's E-Safety Top Tips

Please read the 'Top Tips' which aim to keep us all safe when using the internet

Don't post any personal information online– like your address, email address or mobile number

Don't post any personal pictures or videos of yourself. Once you have put a picture of yourself online most people can see it and maybe able to download it, it's not just yours anymore

Keep your privacy settings as high as possible

Never give out your passwords

Don't befriend people you don't know

Don't meet up with people you have never met online. Speak to your parent or carer about people suggesting you do

Remember not everyone online is who they say they are

Think carefully about what you say before you post something online

Respect other peoples views, even if you don't agree with someone else's views doesn't mean you have to be rude

If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer and tell a trusted adult immediately

APPENDIX D