



# E-Safety Policy

July 2019

Review Date: July 2020

E-Safety Designated Person:

Mrs M Sorensen

Nominated Governor for E-Safety:

Mrs D Williams

This policy must be read alongside the Matrix's Child Safeguarding Policy, Staff Code of Conduct Policy, Behaviour Policy, ICT Acceptable Use Policies and our Anti-Bullying Policy.

This policy has been written in conjunction with the following guidelines: UK Council for Internet Safety (2019) Social Networking, Social Media and Email: Protecting Your Professional Reputation (ASCL Sept 2016)

# 1. INTRODUCTION

## 1.1 What is e-safety?

1.2 Barr Beacon 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.

1.3 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.

1.4 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 Barr Beacon School that 'online actions can have offline consequences'.**

## 3. ACCEPTABLE USE POLICIES (Pupils, Staff and 6<sup>th</sup> Form)

### 3.1 Important information

3.2 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.

3.3 All pupils, students, trainee teachers and staff will be expected to read our ICT Acceptable Use Policies and sign the appropriate consent documentation before an account is created.

3.4 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.

3.5 Further staff guidance for personal use and social networking will be discussed as part of the staff induction process (including NQT and SCITT programmes) 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 and the Staff Code of Conduct*).

### 3.6 Barr Beacon 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.
- The school appoints a member of the Governing Body to take lead responsibility for e-safety.
- A member of school staff will be accredited with CEOP (Child Exploitation and Online Protection) training.
- 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 Lead 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 Child Safeguarding, 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 Children's Services 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 will 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 *"Using the internet, email, online games or any digital technology to threaten, tease, upset or humiliate someone else"* (Childline.org.uk 2018).

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 vulnerable and isolated. This can be harmful, threatening and a great source of anxiety.

4.4 Where bullying outside of school (such as online or via text message / voicemail) is reported to school, it will be investigated, acted upon and recorded in line with our school policies. However, children's use of social media outside of school is parents' responsibility and we advise parents to monitor this closely.

### 4.5 Barr Beacon School 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).
- There are clear procedures in place to support any pupils involved in 'Sexting' (Youth Produced Imagery) incidents (please refer to the school's Child Safeguarding Policy for further information).
- School will consult and refer to agencies where appropriate, i.e CEOP (Child Exploitation and Online Protection), Police, Children's Services where necessary.

## 5. MOBILE DEVICE POLICY

5.1 Barr Beacon School 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 our letter to parents which can be accessed on the school website (**Appendix C**). Please also refer to our Mobile Phone Procedure flow chart which can also be found in our Safeguarding Policy (**Appendix D**).

- 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.

5.2 We ask all visitors not to use their mobile phones on school premises.

## 6. ROLES AND RESPONSIBILITIES

### 6.1 Pupils and Staff MUST:

- Immediately report to **the Designated Safeguarding Lead** if they receive offensive or abusive emails, text messages or posts on social networking sites.
- Immediately report to **the Designated Safeguarding Lead** 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 and ensure security settings are at the highest level of privacy.
- 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 Barr Beacon's Top Tips for E-Safety <http://www.barrbeaconschool.co.uk/wp-content/uploads/2014/10/DL-Top-Tips.jpg> which are displayed around school and can be found on the school website.

## 7. COMMUNICATING E-SAFETY

- E-safety information leaflet for pupils, parents and carers is available on the school website (**Appendix E**).
- Providing 'cyberbullying' government guidance for parents on the school website.
- Guidance and information for parents on e-safety issues are available on the school website and updated regularly.
- E-safety posters with pupils' 'Top Tips' for keeping safe when using the Internet will be displayed in all Form Tutor rooms, ICT rooms, Heads of House offices, Leadership offices and on the e-safety display board and television screens (**Appendix F**).
- 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. Our e-safety working group 'Digital Leaders' work with key staff to share ideas, participate and assist in the delivery of assemblies and actively raise awareness of e-safety in school.
- Regular training and updates (CPD - Continuing Professional Development) will be provided for all staff, raising 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.

- Theatre in Education production companies are invited into school to deliver workshops and raise awareness of issues surrounding 'online grooming', 'sexting' and 'radicalisation'.
- 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 e-safety awareness guidance in newsletters, the school prospectus, and Settling In Evening. E-Safety alert texts are sent to parents to update on possible issues. A Parental platform guide is available on the school website with top tips and updates on social media apps and general safety. This is updated every Wednesday (Appendix G).
- Parents to ensure that contact details are up to date.
- A partnership approach to e-safety at home and at school will be encouraged by offering parental e-safety sessions and guidance via the school website 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](http://www.ceop.police.uk)

Alternatively, click the following link [on our school website](#):



**Useful e-safety websites for further information and guidance include:**

Internetmatters.org: [www.internetmatters.org](http://www.internetmatters.org)  
 Childnet: [www.childnet.com](http://www.childnet.com)  
 UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)  
 Think U Know: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)  
 Childline: [www.childline.org.uk](http://www.childline.org.uk)  
 Parentzone: [www.parentzone.org.uk](http://www.parentzone.org.uk)  
 Get Safe On Line Ltd: [www.getsafeonline.org](http://www.getsafeonline.org)  
 Parent Info: [www.parentinfo.org](http://www.parentinfo.org)  
 National Online Safety: [www.nationalonlinesafety.com](http://www.nationalonlinesafety.com)  
 New Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)  
 NSPCC: [www.nspcc.org.uk](http://www.nspcc.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, Instagram, Snapchat, YouTube, etc) is not disputed, Barr Beacon 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 Barr Beacon 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.
- When using social networking sites, ensure that any profile pictures used are appropriate and that you are not using your full name.
- Choose your friends carefully, not accepting friend requests from pupils, parents or any unknown requests.
- 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 Designated Safeguarding Lead 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
Tellonym	Read what is Tellonym Read what can I do to protect my teenager on Tellonym Report to Tellonym
Tik Tok	Ensure that your child's account is 'private'. Read support.tiktok.com
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



Barr Beacon School  
www.barrbeaconschool.co.uk

Ref: LD/cc/Mobile Phones

June 2019

Dear Parent/Carer

Barr Beacon School is a **NO MOBILE PHONE SITE** for Years 7, 8,9,10 and 11 pupils.

I want to take this opportunity to inform you of the procedure we will follow if your child chooses to break this school rule and bring a mobile phone into school.

The phone will be confiscated immediately and you will be contacted so that a mutually convenient time can be arranged for you to meet with a member of Leadership. This meeting will enable me to ensure that the phone is checked, in your company, for any inappropriate content. The meeting to check the phone will not happen on the day of confiscation. However, we will endeavour to meet you within two weeks of confiscation. If, following this meeting with you, your child brings his/her phone into school again, the phone will be checked again for inappropriate content by a member of Leadership and will remain in the school safe for 6 weeks.

During a most recent incident, several pupils were found with images of other school pupils on their phones and the phones contained photographs/videos that had been taken on school site. If we are to keep your child safe, it is **ESSENTIAL** that no other pupil is allowed to have images of your child in their possession, without your consent.

I would also urge you to read an article printed in the guardian which shows the results of a study by the London school of economics. This study found that pupils at mobile-phone free schools performed better in GCSE examinations and showed a sustained improvement in examination results. This article can be viewed at <http://www.theguardian.com/education/2015/may/15/mobile-phone-bans-improve-school-exam-results-research-shows>

My staff may also be conducting checks to ensure that all pupils are following this most important rule in order to ensure that your child is as safe as possible.

I would urge you to ensure that you know all pass codes for your child's phone and that you are checking this at home on a regular basis. This is deemed to be best practice in terms of keeping children safe as it will enable you to monitor him/her for age inappropriate content and also to monitor the communication your child may be having with others, including any potentially 'risky' adults. Please see our e-safety parental advice leaflet, this can be found under the 'About' then 'Safeguarding' tab on the school website. |

I would ask that you reinforce with your child the need to leave their phone at home and that their phone will not be brought onto Barr Beacon School site and that if they choose to break this rule, you and your child are clear about our procedure.

I thank you again for your continued support in this most important safeguarding matter.

Yours sincerely

Ms L Draycott  
Headteacher

 Barr Beacon School  
Old Hall Lane  
Aldridge  
Walsall  
WS9 0RF  
West Midlands



0121 366 6600

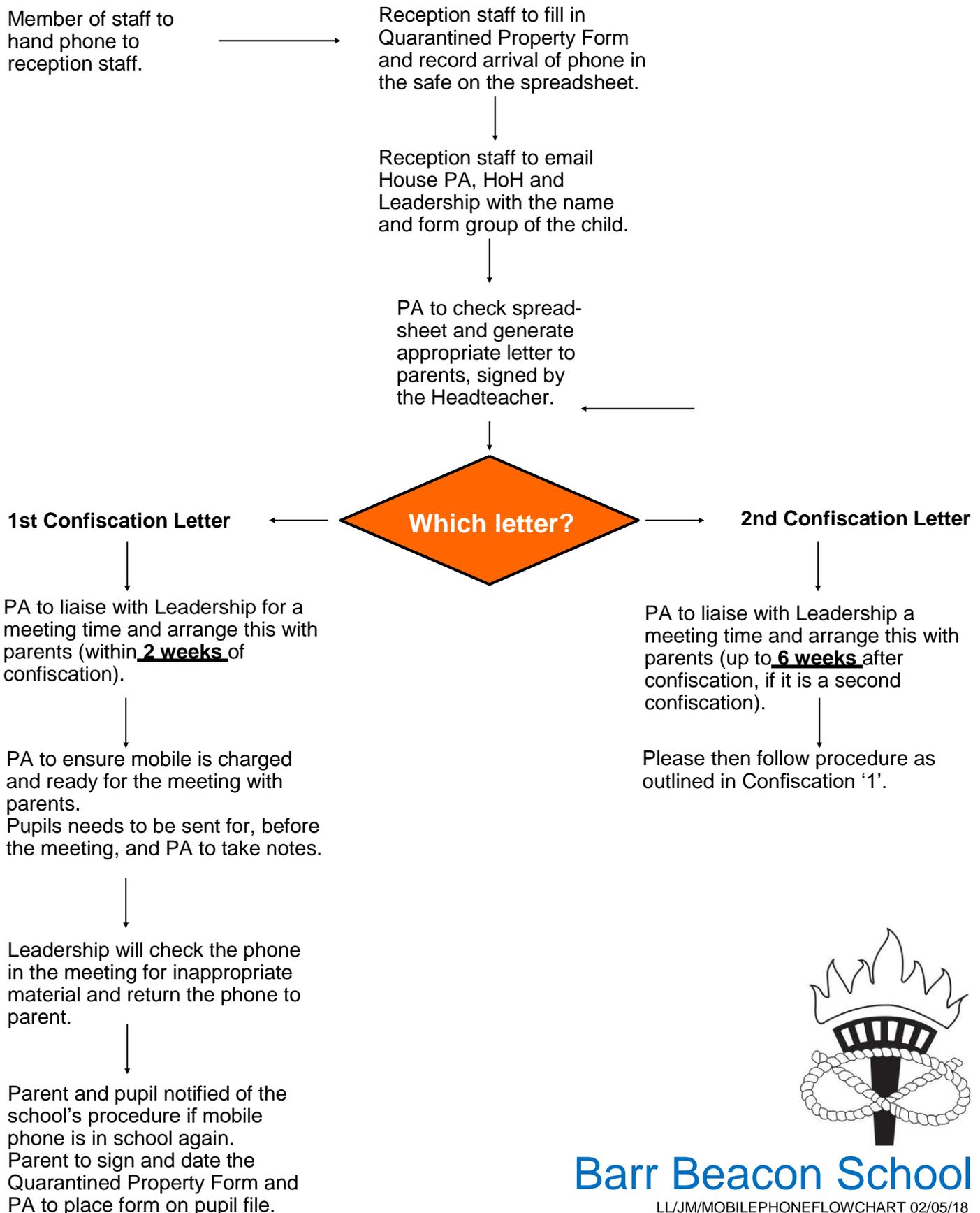
@barrbeaconsch

postbox@barrbeaconschool.co.uk



## APPENDIX D

# Confiscation of Mobile Phone Procedure



# APPENDIX E

## e-Safety Information For Pupils, Parents & Carers



### Why is e-Safety important?

Young people today live in a digital world. At Barr Beacon School, 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 on how to be safe online



postbox@barrbeaconschool.co.uk



@barrbeaconsch



www.barrbeaconschool.co.uk

### How Your Child Uses ICT At Barr Beacon School

ICT is taught as an individual subject, but is also 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 Presentation** (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 and Garageband) to create compositions
- **Coding Software** such as Python

### Our mobile phone policy



Barr Beacon School is a **NO MOBILE PHONE SITE** for Years 7-11.

Our mobile phone policy has been written to ensure that all of 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.

### 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 that 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.

### Advice

- Don't allow your child to take their phone/ laptop to bed with them.
- Check your child's social media apps **regularly**.
- Check the age requirements for all social media apps.
- Check their camera roll and deleted pictures.
- Don't just check what is on your child's monitor.
- Remember that your child is living in a completely different world to when we were in school!
- Click the "**CEOP Internet Safety**" button on the bottom of the Barr Beacon website.



### Recommended websites for further information:



www.ceop.gov.uk



www.thinkuknow.co.uk

# APPENDIX E

## How Can You Help Your Child At Home? Barr Beacon School's Top e-Safety Tips:

ICT is not just about using a computer - it is the use of mobile phones, digital cameras, iPads (tablets, phablets, Kindles, smart watches). 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 **texts, 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.

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

**Do not** upload past images/videos of yourself or others that are inappropriate. You don't know how these images will be used by others!

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

Know your privacy settings. **Do not** give away your location



If you feel unsafe online, tell a parent, carer or teacher and click the report abuse button on the school website. <http://www.barrbeaconschool.co.uk/>

## SAFEGUARDING

AT BARR BEACON SCHOOL

Barr Beacon School is committed to the highest standards in protecting and safeguarding our pupils and students.

Our school will support all pupils and students by:

- Promoting a caring, safe and positive environment
- Encouraging self-esteem and self-assertiveness
- Effectively tackling bullying and harassment

*If you have a concern that any pupil or student is being harmed, is at risk of harm or you receive information (intentionally or unintentionally) you must contact the following designated member of staff as soon as possible:*

Mrs Sorensen

Assistant Headteacher

If this person is not available, please contact Miss Franks (Head of House) or Ms Draycott (Headteacher)

Thank you

BARR BEACON IS A "TELLING SCHOOL"

LC00/SAFEGUARDINGPOSTER19

### Talking with children about "Sexting" (Youth Produced Imagery)

**What is Youth Produced Imagery (Sexting)?**

- Images, videos or text generated by children under the age of 18, that are of a sexual nature.
- If a child under the age of 18 sends a sexually explicit photo to another child, it can be very serious. the child can be charged with possessing and distributing child pornography.
- We strongly advise parents to discuss youth produced imagery with their children as a recent Sky News report stated that '37% of teenager have admitted to sexting, yet 60% of parents have not discussed this issue with their child'.

**For further advice and guidance on e-safety and "sexting" please visit:**

- [www.ceop.gov.uk](http://www.ceop.gov.uk)
- [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
- <https://parentzone.org.uk/>
- <http://www.saferinternet.org.uk/>
- [www.childline.org.uk/](http://www.childline.org.uk/)



# DIGITAL LEADERS TOP E-SAFETY TIPS:

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

**Do not** upload past images/videos of yourself or others that are inappropriate. You don't know how these images will be used by others!

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

Know your privacy settings. **Do not** give away your location



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



<http://www.barrbeaconschool.co.uk/>

# APPENDIX G



**“7 CONVERSATION TOPICS”**  
about Online Safety  
for Parents

Click to download →



**“ONLINE BULLYING”**  
Online Safety Guide  
for Parents

Click to download →



**“SNAPCHAT”**  
Online Safety Guide  
for Parents

Click to download →



**“WHATSAPP”**  
Online Safety Guide  
for Parents

Click to download →



**CATFISHING**  
guide for Parents

Click to download →

