Barrowford Primary School

Learn to Love, Love to Learn

Online Safety Policy

Dated: September 2019 Review Date: September 2020

Reviewed by: Karl Cross

Headteacher: Rachel Tomlinson

1. Barrowford School's vision for Online Safety

Barrowford Primary School strives to provide a diverse, balanced and relevant approach to the use of technology. We ensure that children learn in an environment where security measures are balanced appropriately with the need to learn in a safe environment. The children will be equipped with the skills and knowledge to use technology appropriately and responsibly. We teach skills to recognise the risks associated with technology and how to deal with them, both within or outside the school environment.

In a world where technological advances are moving at a fast pace, ensuring that our children can use technology effectively and safely is of utmost importance. Particularly in regards to online safety.

While there are huge benefits to being online, it is important to be aware that any time children use the Internet, they do face some potential risks, such accessing inappropriate or harmful content, harmful interactions with other users, oversharing their own personal information, grooming and sexual abuse, online bullying, gambling and manipulation by online organisations and radicalisation. We believe educating your child in safe use and understanding what to do in difficult online situations helps keep them safe online.

There are some websites and games that have age restrictions and checks on them to make sure that children don't see unsuitable content. The same goes for social media networks. It is our expectation that children at Barrowford engage safely and appropriately when online and do not have their own social media accounts. This is because children must be at least 13 to register on most social networking websites. However, the reality is there's not a lot standing in the way of children joining at a younger age so it is vital as parents and carers that you really take an interest in your child's online behaviour and have a good overview of how they use their computer or mobile device to ensure they are only accessing content that is appropriate for their age. We believe age restrictions are there for a good reason. We aim to work alongside our school community to ensure that both children are parents have the knowledge, skills and confidence to make the most of the technology available to them.

In this day and age, online safety has to be more than a reminder not to speak to strangers online. As children begin to navigate the internet and use it in different ways as they grow older, their own personal conduct online is also an area where they need guidance. We believe it is important to teach children both about the technological and social and emotional aspects of being safe and successful online.

2. Online Safety Coordinator

The school has appointed Karl Cross as the Online Safety Coordinator.

Responsibilities are:

- Ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of the reporting procedures and requirements should and Online Safety incident occur.
- Ensuring any Online Safety Incidents are recorded on CPOMs
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with national agencies such as the Child Exploitation and Online Protection centre (CEOP)
- Providing or arranging advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, children and governors are updated as necessary
- Liaising with the school's Designated Senior person/Social Worker to ensure a co-ordinated approach across relevant safeguarding areas.

3. Security and data management

In line with the requirements of the Data Protection Act (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's right
- Adequate, relevant and not excessive
- Kept no longer than necessary
- Only transferred to others with adequate protection

All records are the responsibility of SLT. Staff should ensure they are familiar with the Confidentially and Record Keeping Policy.

4. Use of Mobile devices

Staff use

- Staff may use their mobile phones for emergency personal reasons whilst in school. They should however not use them during teaching time.
- No mobile phones should be used in toilets or areas where children may be changing.
- Staff should not speak on their mobile phones in the staffroom when others are trying to relax.
- Mobile phones must be switched to silent during the school day.
- Staff may log on to school Wi-Fi for work related internet use.
- Any images, video or audio recorded must only be on school devices. You must not use your mobile phone or any other personal device.

- Staff must inform Karl Cross if they feel there is suspicious use of mobile phones or cameras by any person in school.
- Staff are responsible for their personal devices. School does not accept responsibility for any breakages to mobile devices.

Pupil Use

- Pupils should not bring their mobile devices into school. However parents may request this for safety reasons – e.g. a child who walks home alone.
- Any pupil bringing a mobile phone into school must have consent of parent and class teacher.
- Mobile devices must be switched off and handed in to the office during the school day.
- Pupils/Parents are responsible for their personal devices. School does not accept responsibility for any breakages to mobile devices.

5. Use of Digital media

Photographs and videos of children and adults may be considered as personal data in terms of the Data Protection Act (2018).

Consent and Purpose

- School must gain consent from parents for photographs of their children to be taken or used. This must be recorded on SIMs. Parents must be made aware of how photographs could be used. E.g. on Facebook, Twitter, School Website, You tube, assessment tools, brochures or displays. The school office will have a record (available via SIMs) of any pupils who do not have consent.
- Permission should be obtained when children start school; however parents may request permission removal whenever they feel is appropriate.
- Any pupil who does not have consent for photographs must not be used for press purposes.

Taking Photographs/Video

- Any member of staff wishing to take images of children must be approved by the headteacher
- Photographs must not be taken on any personal devises – school iPads / iPods are provided in each classroom
- No pupils should be continually favoured in images
- Close up shots should be avoided as these may be considered intrusive. Shots should preferably include a background context in group situations

Parents Taking Photographs/Videos

Under the Data Protection (2018), parents are entitled to take photos of their own children on the provision that the images are for their own use, e.g. at a school production. We ask that any images in which other children are visible are not shared on any social media platform. Including other children or purpose could constitute a potential breach of Data Protection legislation.

- Parents should be advised to only photograph their own children at events.

- Parents need to be reminded that publishing images which include other children than their own or adults on Social Networking sites are not acceptable, unless specific permission has been obtained from the subjects.
- Parents should be encouraged to be considerate when taking photographs e.g. not obscuring the view of others or being intrusive.

Storage of Photographs/Videos

- Any photographs taken may be uploaded to teacher's school laptops. Laptops must be password protected.
- Images must be deleted from school iPads/IPods. Any images or videos that need to be stored must be uploaded to teacher laptops.
- Any images stored on 'Clouds' must be password protected.
- Staff must not store personal images on school equipment.
- Class teachers have responsibility for deleting images from iPads/IPods. Karl Cross will monitor this.
- No images should be 'sent' electronically without a secure account.

Publication of Photographs/Videos

- Consent is needed from parents for publication of children's images e.g. on a website.
- Photographs should only be published online to secure sites.
- Names or other personal information should not accompany published images.
- Staff should not post images on personal Social Networking sites.

The Media 3rd Parties and Copyright

All 3rd Parties must be supervised at all times whilst in school and must comply with the Data Protection Requirements in terms of taking, storing and transferring images.

CCTV, Video Conferencing, VOIP and Webcams

- Parents should be informed if CCTV, video conferencing and webcams are being used in school.
- Only pupils who have parental consent may appear on video conferencing links

6. Communication Technologies

Barrowford School uses a variety of communication technologies and is aware of the benefits and associated risks. As new technologies are introduced this policy will be updated and all users made aware of the changes.

Email

- All staff should use their professional @barrowford.lancs.sch.uk accounts to communicate. All email should contain the following disclaimer - *This communication is from Barrowford Primary School, and contains information that is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any form of use, dissemination, distribution, copying or printing of this*

communication or the information in it is strictly prohibited and may be unlawful. If you have received this communication in error, please return it with the subject 'received in error' to the sender then delete the email from your system and destroy any copies of it.

- On some occasions email may be used as a learning tool with children. Any accounts should be set up by the class teacher. No pupil should be identified through an email account – they should be class, phase or project accounts. All emails received and sent should be monitored by the class teacher. Pupils must be taught how to report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks

Popular examples of Social Networks include Facebook, Twitter, and Instagram. They all allow users to be part of a virtual community. Although use of Social Networks tends towards a personal basis outside the school environment, they are also used in school as a tool to communicate with parents.

All staff must be mindful of the following points:

- All staff that use professional Social Networking accounts should ensure that all communication with parents is only linked to school.
- Professional accounts should always have high security settings. Photographs added must be only be seen by 'friends'.
- If a Social Network site is used personally, details should not be shared with children and parents. Privacy settings should be reviewed regularly to ensure information is not shared automatically with a wider audience than intended. Staff should not make friends with parents or children on personal accounts.
- On any account staff should not give personal contact details.
- The content posted online should not:
    - Bring the school into disrepute
    - Lead to valid parental complaints
    - Be deemed as derogatory towards the school and/or its employees
    - Be deemed as derogatory towards pupils and/or parents and carers
    - Bring into question their appropriateness to work with children and young people.
- Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- Children must not be added as 'friends' on ANY Social Networking site.

Barrowford School will work with parents in terms of advice they give in terms of their use of Social Networking Sites. Concerns may include:

- Posting inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- Posting images of children on profiles without permission of the individuals involved, especially if the photograph contains children other than their own.

Instant Messaging

Instant Messaging systems e.g. Text messaging, Skype, Facetime, are popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video.

- Staff should not share mobile numbers with Parents or children
- Staff should not use school equipment to communicate with personal contacts e.g. through 'Facetime' on an iPad.

Microsoft Teams

- As a school we have set up Microsoft Teams to allow for continued communication between school, pupils and their families during exceptional circumstances whereby school is closed for an extended period of time.
- As part of this process all of the pupils in school have had a school email address set up for them. As a result the pupils and their parents have access to communication from school via, video and/or audio calls and through emails and messaging on the teams platform.
- Video/audio calls should be made to 'check in' with how pupils and their families are managing extended periods of school closure.
- Staff should only video/audio call a pupil if more than one member of staff is present in the chat or if the parent of the child is present to ensure the safety of both staff members and pupils. Alternatively staff can record calls to ensure that the conversations that take place are safe and appropriate. These recordings are to be made on school allocated laptops that are encrypted following GDPR guidelines and safeguarding processes.
- If a one to one call is required to help a pupil with learning then this needs to be prearranged with the parent for a specified date and time with that parent also present.
- If a member of staff, pupil or parent has any safeguarding concerns following a video/audio call then they are to follow school's policy and procedures regarding safeguarding, referring those concerns immediately to the DSL or a deputy if the DSL is unable to be contacted.
- Staff are to make clear to pupils and parents acceptable use for Microsoft Teams relating to school's online safety policy. Any inappropriate content is to be challenged by staff and parents contacted to inform them of this.
- Parents need to also be asked at the request of the staff members to check the chat messages of their child(ren) to ensure that content is appropriate and that any conversations that are being engaged in (whether with staff members or other pupils) are safe and appropriate.

7. Websites and other online publications

Information posted online is readily available for anyone to see and thus form an opinion about the school. The School Information (England) Amendment Regulations 2016 specify that certain up to date information must be made available on a school's website.

- The school website should have information that communicates Online Safety messages to parents
- Karl Cross and Glyn Wilson have access to edit online publications and ensure that the content is relevant and current.
- All downloadable materials should be in PDF form to prevent content being manipulated and potentially redistributed.

8. Infrastructure and Technology

Dated: September 2019 Review Date: September 2020

Reviewed by: Karl Cross

Headteacher: Rachel Tomlinson

Children's access

- Children should always be supervised when accessing school equipment and online material
- Children have class logons to gain access to the school system.
- Certain areas are restricted to children such as documents on 'the blackboard' that are confidential.

Passwords

- All users of the school network have a secure username and password.
- The administrator password is held by Glyn Wilson.

Software/Hardware

- School has legal ownership and licences for all software.
- Software installation is controlled by Glyn Wilson.

Managing the network and technical support

- All wireless devices are security enabled.
- All iPad/iPod have had 'App store' disabled. Jonny Savage has the password and can install and delete apps.
- All staff are responsible for the security of the network. Any security risks should be reported immediately to Glyn Wilson.
- All computers are updated with Sophos through the server.
- All staff and children have defined access rights to the network. This is managed by Glyn Wilson.
- Staff can download software onto their staff laptops. Children do not have access to this.
- If there is a breach of security it must be reported to Karl Cross.
- Karl Cross to liaise with Glyn Wilson with regard to the computer network.
- All external visitors to use the visitor Wi-Fi network. The username and password is available from the office staff.

The Sonic wall Firewall sits between the school network and the internet. It does the following:

- Protects the school from attacks from the internet
- Blocks access to certain categories of websites in school, for example, weapons, pornography, social networking. We can control on the firewall what types of categories are blocked and also give teachers different access to pupils.
- Staff are aware that no firewall is ever 100% effective. For example a certain trustworthy site might happen to contain an article that may be unsuitable for pupils, BBC News for example may contain some content from time to time that might be deemed unsuitable for Early Years pupils.

9. **Dealing with Incidents**

All Online Safety incidents should be recorded on CPOMs under E-Safety. This must be audited termly by Karl Cross and other members of the SLT

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the head teacher who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation. **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Always report illegal content to the Internet Watch Foundation (http://www.iwf.org.uk)

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

Inappropriate Use

Listed in the table below are examples of possible inappropriate use and procedures to follow up incidents.

Incident	Procedure
Accidental access to inappropriate materials	• Minimise the webpage. • Tell a trusted adult. • Enter the details in the Incident Log and report to Glyn Wilson for filtering .
Deliberate searching for inappropriate materials. Bringing inappropriate electronic files from home Using chats and forums in an inappropriate way.	• Inform SLT or designated Online Safety Champion (Karl Cross). • Enter the details on CPOMs. • Additional awareness raising of Online Safety issues and the AUP with individual child/class. • Consider parent/carer involvement.

10. Education and Training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

The three main areas of Online Safety risk (as mentioned by Ofsted, 2013) that staff need to be aware of and consider are:

Area of Risk	Example of Risk
Content: Children need to be taught that not all content is appropriate or from a reliable source.	• Exposure to inappropriate content, including online pornography, ignorig age ratings in games (exposure to

	violence associated with often racist language), substance abuse. • Lifestyle websites, for example pro-anorexia/self-harm/suicide sites. • Hate sites. • Content validation: how to check authenticity and accuracy of online content.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming • Cyberbullying in all forms • Identity theft (including 'frape' - hacki ng • Facebook profiles and sharing passw ords.
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	• Privacy issues, including disclosure of personal information, digital footpri nt and online reputation • Health and wellbeing - amount of time pent online (internet or gaming). • Sexting (sending and receiving of per sonally intimate images). • Copyright (little care or consideration for intellectual property and ownership, such as music and film).

Online Safety – Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' Online Safety.

- Online Safety should be planned into teaching as often as possible in all year groups.
- There should be a half termly Online Safety day.
- All children need to be made aware of the impact of cyberbullying and how to seek help if they are affected by these issues.
- Pupils should be taught to critically evaluate materials and develop good research skills.
- Online Safety rules should be displayed in every classroom

Online Safety – Raising staff awareness

- Staff training needs should be audited yearly to ascertain the level of knowledge and expertise in the use of new technologies and their potential benefits and risks.
- Staff should receive Online Safety training annually.
- Karl Cross will provide advice/guidance or training to individuals as and when required.
- Online Safety training should also include information which may affect their own personal safeguarding e.g. use of Social Networking sites.

- All staff are expected to promote and model responsible use of ICT and digital resources.

Online Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

- Information regarding Online Safety will be added and regularly updated on the school website
- Parents Online Safety workshops will be held
- School will promote external Online Safety resources/online materials

Online Safety – Raising Governors' awareness

Online Safety updates will be reported through the Behaviour and Safety Committee.