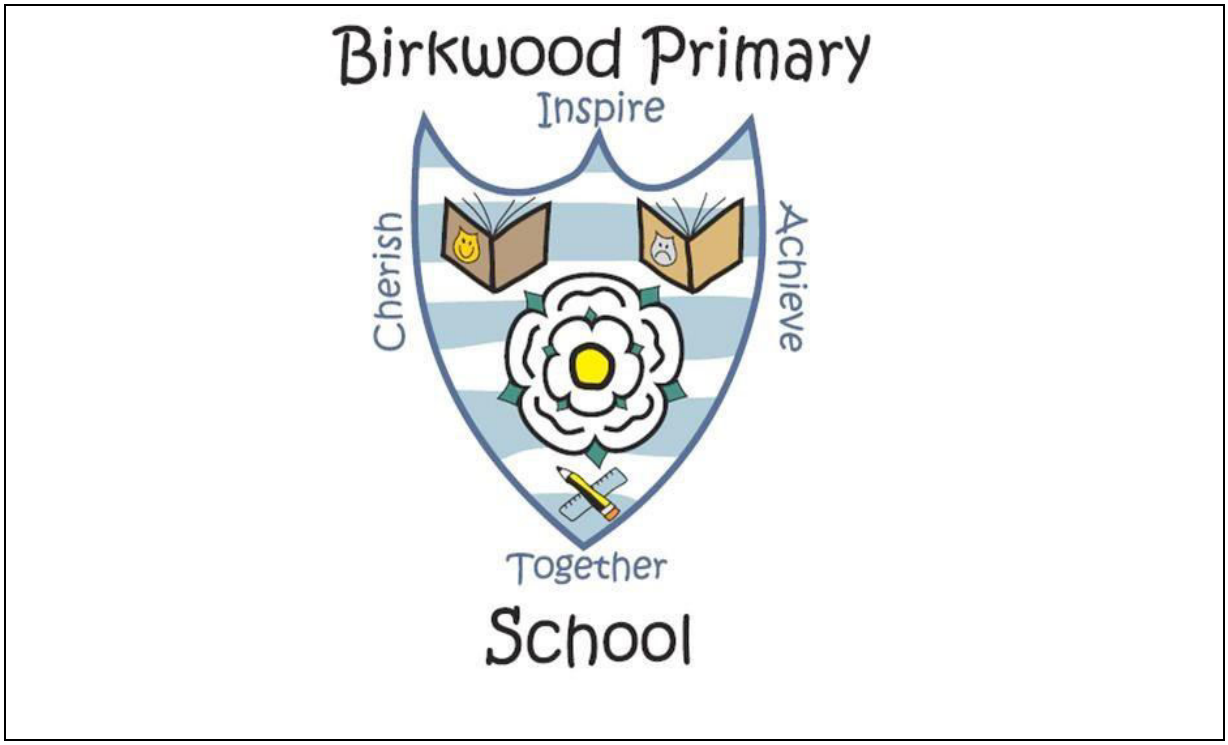

ONLINE SAFETY POLICY

JANUARY 2022

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites – individual logins for PurpleMash, Spelling Shed and TT Rockstars
- Learning Platforms and Virtual Learning Environments – Class Dojo and Microsoft Teams
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting/ Streaming
- Music Downloading/ Streaming
- Gaming
- Mobile/Smart phones with text, photo, video and/or web functionality
- Other mobile devices (including e-Readers) with web functionality
- SMART Televisions

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources and social networking apps, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Birkwood Primary School, we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is written in conjunction with the school's Safeguarding and Child Protection Policy, Website Policy and Twitter Policy. The policy is inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, tablets, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, smartphones, tablets and portable media players, etc).

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinators in our school are Mr. Ben Froggatt, who has been designated this role as Safeguarding Lead, and Mr. Niall Sandwith, who has been designated this role as part of his Teaching and Leadership Responsibility. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance.

The e-Safety coordinator updates Senior Management and Governors and all have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the e-Safety policy

This policy, for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for ICT, Home-school agreements, Behaviour, Health and Safety, Safeguarding and Child Protection, PSHE policies including Anti-bullying and eBehaviour agreements.

Our e-Safety policy has been written by the school, in conjunction with advice from Barnsley Metropolitan Borough Council, has been agreed by the Senior Leadership Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues through the coordinator at staff meetings, in order to improve staff knowledge of, and expertise in, safe behaviours and appropriate use of technologies.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (log on CPOMS and tag with 'e-safety).
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.
- An Online Safety Training Needs Audit is completed annually which will inform future training (see Appendix 1)
- Training for staff takes place annually following an audit of the needs of all staff.

E-Safety information for parents/carers

- Parents/carers are made aware that their child will agree to an eBehaviour agreement ~ these are appropriate to EYFS, Key Stage 1, 2 and Parents/Carers (see Appendix 2,3 and 4).
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school's website/ social media account(s). This is in conjunction with Section 9 (Photographing Children) of the school's Safeguarding and Child Protection Policy.
- The school website contains useful information within its Parentzone tab, and includes links to sites like Thinkuknow, Childnet, CEOP, and Internet Matters.
- The school will send out relevant e-Safety information through newsletters, the school website, School Twitter accounts and the School Prospectus.

Community use of the Internet

A guest network has been set up, and external organisations using the school's ICT facilities must adhere to the e-Safety policy.

<u>Teaching and Learning</u>

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas and assemblies to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them (in conjunction with the school's Anti-Bullying Policy). Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Filtering will be managed by Code Green after liaisons with E-Safety co-ordinator.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be educated in protecting personal information and using strong passwords when accessing the internet – passwords will become gradually stronger as children progress through school

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information System Security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Code Green.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school website

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website (see Appendix 5). This consent form is considered valid for the current academic year unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully with consideration to safeguarding issues.
- Pupils' full names will not be used anywhere on the Birkwood Primary School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Social networking and personal publishing

- Code Green will block / filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them. They will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying or peer-on-peer abuse to the school.
- School staff are advised to check their privacy settings are secure and not to add children as 'friends' or accept them as followers if they use these sites.

Managing filtering

- The school will work with the LA and Code Green to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher, e-Safety Coordinator or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material. Encrypted memory sticks must be used by staff for use at home in line with GDPR. Staff can access the school's network remotely through Forticlient which is password protected; staff must ensure their devices are locked when they are absent from it.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school are handed to the class teacher to be kept safe until the end of the day. Mobile phones must be switched off at all times when on the school premises, unless express permission has been given by a member of staff.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with pupils is required e.g. on trips and visits.
- Staff should not use personal mobile phones during designated teaching sessions unless they are taking photos as evidence of learning to be used on Twitter/Website.
- Staff are aware that all images must be deleted from personal devices once they are uploaded.

Managing emerging issues

Birkwood Primary School is committed to a whole-school, zero-tolerance approach against Peer-on-peer abuse (see Appendix 7). When managing emerging issues (some of which are referenced in Appendix 6), the IT co-ordinator and Designated Safeguarding Lead will seek relevant advice from the government and/or appropriate body to ensure appropriate action is taken in order to prioritise the safety and wellbeing of the child/young person.

Protecting personal data

The school will collect personal information about you fairly and will let you know how the school and Barnsley LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or

Barnsley LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Barnsley LA.

The school will hold personal information on its systems in line with retention policies. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Barnsley Metropolitan Borough Council and as defined by the Data Protection Act 1998 and GDPR from 25th May, 2018.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the eBehaviour Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all classrooms and on device trolleys.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- All parents will be provided access to the eBehaviour Agreement for pupils for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's Online Safety policy.
- All staff must read and agree in writing to adhere to the Information Security Policy for staff before using any school ICT resource.

Password Security

- Adult users are provided with an individual network and email password which they are advised to change every 63 days.
- Staff are advised to write a password that is at least 9 characters long and contains numbers, special characters and capital letters.
- Accounts will be locked out following 5 failed attempts until an administrator unlocks the account.
- All pupils are provided with an individual network login, and email when appropriate.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware that their screens should be locked when unattended; a password lock screensaver should be set at a reasonable working time (e.g. 15 minutes).
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BMBC can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator and recorded in the e-Safety incident Management Log.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the E-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year.
- All pupils sign an e-behaviour agreement at the start of the academic year (Appendix 2,3 and 4).
- Specific lessons will be taught by class teachers as part of the computing curriculum and at relevant points throughout e.g. during PSHE lessons/circle times/Safer Internet Day/anti-bullying week/half-termly assemblies.
- Pupils will be informed that network and Internet use will be monitored**.**

Staff and the e-Safety policy

- All staff will have access to the school's Online Safety policy through the shared drive and the school's website.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware when emailing any files containing personal data, they must be sent in an encrypted manner.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The Headteacher, Designated Safeguarding Lead and IT co-ordinator will be alerted via email (through Netsweeper reporting**)** of any inappropriate Internet searches or visited websites on any school device.
- A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.
- Staff should be mindful that an online reputation is important for current and future employment (See Appendix 1 of Staff Handbook and BMBC Social Networking Policy).

Monitoring and Review

The Governing Body reviews this policy every year. The Governors may, however, review the policy earlier than this, if the government introduces new regulations, or if the governing body receives recommendations on how the policy might be improved.

This policy will be reviewed in January 2023.

Signed _____Headteacher Date _____

Signed _____Chair of Governors Date _____

Appendix 1: Online Safety Training Needs Audit

Online Safety Training Needs Audit

1. Do you know the name of the person who has lead responsibility for online safety in school?

Enter your answer

2. Do you know what you must do if a pupil approaches you with a concern or issue?

Enter your answer

3. Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?

- Yes
- No

4. Are you familiar with the school's acceptable use agreement for pupils and parents?

- Yes
- No

5. Do you regularly change your password for accessing the school's ICT systems?

- Yes
- No

6. What is the school's approach to tackling cyber bullying?

Enter your answer

7. What is the school's approach to tackling peer on peer abuse?

Enter your answer

8. Please comment any areas of online safety in which you would like training/ further training.

Enter your answer

Appendix 2: Foundation Stage eBehaviour Promise 2021

Foundation Stage eBehaviour Promise 2021

At Birkwood Primary School you will have the chance to learn in exciting ways. The computers and other exciting equipment will be a part of this learning and we want you to use it safely at all times. We'd like you to listen carefully to this information and write your name at the bottom to show that you know the rules and will be safe and sensible when using the equipment.

eSafety Golden Rules✓	eSafety Golden Rules **x**
Talk to each other kindly. Tell an adult if you see anything you are unsure about including: - iPads or computers that are broken - Pictures that make you sad Tell an adult if someone is being unkind, whether it is to you or others. Always follow instructions when using a computer.	Don't talk to strangers online. Don't share any information such as your name or where you are. Don't be unkind to others.
If you're not sure ASK AN ADULT!	If you're not sure ASK AN ADULT!

Foundation Stage
eBehaviour Promise

I know that school has to keep everybody safe so I will:

- tell an adult if any equipment is damaged or not working properly.
- not change computer settings unless an adult tells me to.

eBehaviour Promise
I promise that I will follow the eSafety Golden Rules. This will keep me and everyone I know safe when using the computers and other equipment.

Name:

Signed

Appendix 3: Key Stage 1 eBehaviour Promise 2021

Key Stage 1 eBehaviour Promise 2021

At Birkwood Primary School you will have the chance to learn in exciting ways. The computers and other exciting equipment will be a part of this learning and we want you to use it safely at all times. We'd like you to listen carefully to this information and write your name at the bottom to show that you know the rules and will be safe and sensible when using the equipment.

eSafety Golden Rules✓	eSafety Golden Rules x
Treat your password like your toothbrush – don't share it with anyone or try to use anyone else's password. Be polite and responsible when communicating with others. Tell an adult if you see anything you are unsure about including: - damage to equipment - upsetting images or text - websites that are not allowed Report bullying whether it is to you or others including: - online bullying - email bullying - text bullying Always follow instructions when using a PC or other technology. If using Social Media, please ensure parents/carers are aware and supervise use.	Don't talk to strangers online ~ remember not everyone is who they say they are. Don't share any personal information such as your full name, date of birth, or address. Never agree to meet with anyone in person that you have met on line. Don't use school equipment for personal use unless you have permission from a teacher. Don't upload or download files that may be upsetting to others. Never open attachments unless you know who sent them. Don't be a bully. That includes verbally, physically or with technology such as the internet, email or mobile phones.
If you're not sure ASK AN ADULT!	If you're not sure ASK AN ADULT!

Key Stage 1 eBehaviour Promise

I know that school has to keep everybody safe so I will:

- tell an adult if any equipment is damaged or not working properly.
- not change computer settings unless an adult tells me to.
- not bring mobile devices to school.

eBehaviour Promise
I promise that I will follow the eSafety Golden Rules. This will keep me and everyone I know safe when using the computers and other equipment.

Name:

Signed

Appendix 4: Child/ Young Person (Key Stage 2) eBehaviour Agreement 2021

Child / Young Person eBehaviour Agreement

At Birkwood Primary School you will have the opportunity to learn in exciting ways. The internet and other technologies will be a part of this learning and we want you to use it safely at all times. We'd like you to sign this form to show that you agree to work safely when using ICT.

This eBehaviour Agreement will help:

- you to be a sensible user of the internet and other communications technologies.
- by providing a secure system across school that helps to protect you as a user.

eBehaviour Agreement

I agree that I will follow the eSafety Golden Rules. This will keep me and everyone I know safe when using the internet and other communication technologies.

eSafety Golden Rules ✓	eSafety Golden Rules **x**
Treat your password like your toothbrush – don't share it with anyone or try to use anyone else's password. Be polite and responsible when communicating with others. Tell an adult if you see anything you are unsure about including: - damage to equipment - upsetting images or text - websites that are not allowed Report bullying whether it is to you or others including: - online bullying - email bullying - text bullying Always follow instructions when using a PC or other technology. If using Social Media, please ensure parents/carers are aware and supervise use.	Don't talk to strangers online ~ remember not everyone is who they say they are. Don't share any personal information such as your full name, date of birth, or address. Never agree to meet with anyone in person that you have met on line. Don't use school equipment for personal use unless you have permission from a teacher. Don't upload or download files that may be upsetting to others. Never open attachments unless you know who sent them. Don't be a bully. That includes verbally, physically or with technology such as the internet, email or mobile phones.
If you're not sure ASK AN ADULT!	If you're not sure ASK AN ADULT!

Key Stage 2
eBehaviour Agreement 2021

I know that school has to keep everybody safe so I will:

- only use USB devices if I have permission.
- respect the filtering systems in place to keep me safe at school.
- tell an adult if any equipment is damaged or not working properly.
- only open emails from people I know.
- not alter computer settings unless an adult tells me to.
- only use chat and social networking sites with permission and at the times that are allowed.
- take care to check that the information that I access is accurate, as I understand that the work of others may not be correct.
- not bring mobile devices to school.

I understand that I am responsible for my actions and that if I break the eSafety Golden Rules:

- I may not be able to use certain ICT facilities within school.
- My parents/carers will be informed.
- The police could be involved if my actions are illegal.

Please sign below to show that you have read and understood the eBehaviour Agreement and agree to the Golden Rules when:

- using the school's ICT systems and equipment (at any time)
- using my own equipment (when allowed) e.g. cameras, USB memory port etc
- using my own equipment at any time in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing email, website etc.

Name of Child / Young Person	
Group / Class	
Signed	
Date	

Appendix 5: Visits and Media Permissions 2021/22

BARNSLEY
Metropolitan Borough Council

Birkwood Primary School
Headteacher: Mr. Daniel Wood
Deputy Headteacher: Mr. Ben Froggatt
Darfield Road, Cudworth, Barnsley
South Yorkshire S72 8HG.
Telephone: Barnsley (01226) 710447
www.birkwood.org.uk
twitter.com/BirkwoodPrimary

16th September 2021

Dear Parents/Carers,

At the beginning of each new school year we like to renew certain permissions, eg. visits, media postings etc.

I am writing to ask you to complete the permission slip, on the other side of this letter, which will cover the year from September 2021 to July 2022. If these permissions change, it is your responsibility to inform school.

Visits in the Local Area

Throughout the school year there will be different opportunities for your child to visit various places in our local area, for example, the Library or St. John's Church.

We will always let you know when we plan an educational visit within walking distance of our school, but by completing the slip overleaf, we would not need to ask you to complete a new letter for each visit.

Media Permissions

At Birkwood Primary School we like to celebrate the achievements of our children and take every opportunity to maximize the impact of these success stories through the use of our Website, Twitter and the local media using photographs and recordings. To comply with GDPR, parents/carers now need to opt into or out of our media celebrations.

With many thanks for your continued support,

Mr Daniel Wood
Headteacher

Visits & Media 2021 / 22

Visits in the Local Area

I do / do not give permission for my child(ren) to go on school educational visits within the local area, that are within walking distance from school.

My child(ren) _____ in class _____

_____ in class _____

_____ in class _____

Media Permissions

If you give your consent your child(ren) may be included in any of the following:

- Photo Displays in and around school.
- Reception Powerpoint
- Website: Birkwood.org.uk including Vimeo
- Twitter: @BirkwoodPrimary
- Class Photos
- Media including Newspapers and Television – Parents/Carers will be notified when there are any planned media events

Without this consent we will not be able to include your child(ren) in any of our success stories.

I have read and understand the above statement.

☐ I give my permission for my child(ren) to be included in media celebrations

☐ I do not give my permission for my child(ren) to be included in media celebrations.

My child(ren) _____ in class _____

_____ in class _____

_____ in class _____

Signed _____
Parent/Carer

Appendix 6: Online safety (from Safeguarding and Child Protection Policy)

This section should be read alongside the school's E-Safety policy and the below online links:

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

At Birkwood Primary School, we recognise, as stated in the January 2021 update to Keeping Children Safe in Education',

> '*that the use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm'.*

Our effective approach to online safety empowers staff to protect and educate the whole school community in the use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. This approach is underpinned by our whole school ethos towards online safety and the ever changing online domain(s).

The breadth of online issues/risks are considered and in particular the three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

We will do everything reasonably possible to limit children's exposure to the above risks from the school's IT systems and ensure we have appropriate filters and monitoring systems in place. In addition, we will consider how IT is a valuable tool for learning and manage the exposure to IT for educational benefit vs. harmful content. School will educate children regarding harmful online content and how to respond to such instances both in school and at home, in an age appropriate manner. Thereby school are not "over blocking", potentially leading to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

School also recognise that whilst filtering and monitoring is an important part of the online safety picture, it is only one part. We also pay close consideration to the whole community approach to online safety. This includes a clear policy on the use of mobile technology in school and also considers that many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G - school carefully considers how this is managed within school and how parents/carers can support their children at home. Should any incidents arise that are considered to be of a cause for concern and/or safeguarding nature, school will manage these incidents on an individual basis and in the appropriate way dependent on individual factors (including if there has been episodes of sexual harassment). These incidents will be managed, monitored, recorded and followed up as detailed in other sections of this policy. This includes supporting any child who has suffered from an incident and/or who needs support either from a victim or perpetrator perspective. When an incident involves sexual violence and/or sexual harassment school will also follow the guidance detailed within Part five of Keeping Children Safe in Education 2021: child on child sexual violence and harassment and Sexual violence and sexual harassment between children in schools and colleges, May 2018.

School provide support for children and parents/carers when learning online using the advice to support schools:

https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

Another element that has become prevalent is harmful online challenges and online hoaxes. ‘A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.’

An online challenge will generally involve users recording themselves taking a challenge and then distributing the resulting video through social media sites, often inspiring or daring others to repeat the challenge. Whilst many will be safe and fun, others can be potentially harmful and even life threatening.

In response to information about an online challenge or hoax, school will use a case-by-case assessment, establishing the scale and nature of the possible risk to children and young people, including considering (where the evidence allows) if the risk is a national one or whether it localised to the area, or institution.

School will use online safety protocols to ensure children are not exposed to such risks, including what they should do/who they should speak to, should they come across such content whether in school or at home. By doing this and using a case-by-case assessment, school carefully consider if a challenge or scare story is a hoax.

In dealing with any online challenge or hoax school will use the following advice:
https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes

Appendix 7: Peer-on-Peer Abuse

Children can abuse other children. This is generally referred to as peer-on-peer abuse and can take many forms. Birkwood Primary School has a zero tolerance policy towards peer-on-peer abuse and never perceives it as 'just banter' or 'having a laugh'. This can include (but is not limited to) bullying (including cyberbullying); sexual violence and sexual harassment; physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm; sexting and initiating/hazing type violence and rituals. Staff are aware that children can abuse other pupils, including through:

- Bullying (including cyber-bullying)
- Physical abuse
- Sexual violence and sexual harassment
- Upskirting
- Sexting
- Initiation/hazing type violence and rituals

The signs of peer on peer abuse can be:

- absence from school or disengagement from school activities
- physical injuries
- mental or emotional health issues
- becoming withdrawn – lack of self esteem
- lack of sleep
- alcohol or substance misuse
- changes in behaviour
- inappropriate behaviour for age
- abusive towards others

To prevent peer on peer abuse at Birkwood we create an environment based on equality and informed choice allowing children to know their rights and what to do if they are unhappy about something. We understand our local community and the context in which children and young people at our school are growing up.

We ensure children know the risks by talking about peer on peer abuse in an age appropriate way. Staff create opportunities for children to weigh up risks and recognise that sometimes this means they will take risks we as adults and professionals disagree with. Our role is to encourage children to make the healthiest long-term choices and keep them safe from harm as far as possible. This in turn also gives children the opportunity to share any episodes of peer-on-peer abuse and feel confident the matter will be taken seriously.

We actively encourage safe relationships with their family, their peers and with staff, through an environment where it is OK to talk, even about the most difficult things.

Staff are aware of the signs and know what to do – recording and acting on information following safeguarding procedures and are confident to raise peer-on-peer abuse as a possibility, however are also aware that just because none has been reported – this doesn't mean it isn't happening. Each individual case will be managed, monitored, recorded and followed up as detailed in other sections of this policy. This includes supporting any child who has suffered from an incident and/or who needs support either from a victim or perpetrator perspective. When an incident involves sexual violence and/or sexual harassment school will also follow the school's Sexual Violence and Sexual Harassment Policy and guidance detailed within Part five of Keeping Children Safe in Education 2021: child on child sexual violence and harassment and Sexual violence and sexual harassment between children in schools and colleges, May 2018.