Broxbourne CE Primary School, EYFS & Extended Schools (Voluntary Aided)

Online Safety Policy

Ratified by Governors:	**November 2023**
Date for Review:	**November 2026**
Signed Chair of Governors:	

Dream, Believe and Achieve with God

Contents

1. Introduction

Broxbourne CE Primary School recognises that internet, mobile and digital technologies provide a good opportunity for children to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success is highly likely to be dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** children, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some children may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. Responsibilities

The Headteacher and Governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety co-ordinator in this school is Paul Miller. All breaches of this policy must be reported to Paul Miller. All breaches of this policy that may have put a child at risk must also be reported to the DSP, Paul Miller.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when children are on site in the care of the school, then the safeguarding of children is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy

The policy applies to:

- children
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that children who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the website, in

newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online. Parental Online Safety Workshops are offered to parents on an annual basis.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, health and safety, home learning, home–school agreement and behaviour policy.

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for children, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account (with Multi Factor Authentication enabled on their devices) or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under **no circumstances** should staff contact children, parents or conduct any school business using a personal email address. Children may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the child's account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and children should not open emails or attachments from suspect sources and should report their receipt to Paul Miller/Emily Andrews/Joanna Davidson and the Data Protection Officer/Deputy Data Protection Officer.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- We use an online cloud software monitoring system called SENSO. This software monitors all desktops and school laptops to identify keystrokes and the use of bad language or words. The software logs these breaches against the specific username and computer. It immediately takes a screenshot of the offending word and is stored for management review. The Headteacher checks SENSO on a termly basis.

- Herts for Learning also filter and monitor our systems and notify the Headteacher where appropriate.

- Staff must preview sites, software and apps before their use in school or before recommending them to children. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with Janet

Boguzas the Data Protection Officer (DPO)/Mary Jaques, Deputy Data Protection Officer with details of the site/service and seek approval from a Senior Leader. The terms and conditions of the service should be adhered to and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online content.

- When working with children searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- adult material that breaches the Obscene Publications Act in the UK

- promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- promoting hatred against any individual or group from the protected characteristics above

- promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

Reveal or publicise confidential or proprietary information

Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses

Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school

Use the school's hardware and Wi-Fi facilities for running a private business

Intimidate, threaten or cause harm to others

Access or interfere in any way with other users' accounts

Use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device. Such a system would ensure the user was not saving files locally to their own device and breaching data security.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Paul Miller, Headteacher.

Storage of Images

Photographs and videos provide valuable evidence of children's achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of children are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the Headteacher, Deputy Headteacher, Data Protection Office (DPO) and Deputy Data Protection Officer (DDPO). Staff and children may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with children, must only use school equipment to record images of children whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of children. Under no circumstance does the school allow a member of staff to contact a child or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is pre-specified permission from the Headteacher or Deputy Headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Children in Year 5 & 6 and lone walkers are allowed to bring mobile phones to school but must not use them during the school day. They also need to complete the Mobile Phone Agreement. Phones must be switched off and remain in their school bag. Under no circumstances should children use their mobile phone to take images of:

- any other child unless they and their parents have given agreement in advance;
- any member of staff.

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles may be used to access school emails and data. Emails can only be accessed via approval from the Authenticator app, either via Face ID on the app or by requesting a code via text message. Please ensure your device is secured by either a password, pin code or face/touch id. Never leave your device with the application open. It is the responsibility of the member of staff to ensure their virus protection software is up to date.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, children and staff should not assume that new technological devices will be allowed in school and should check with the Headteacher, Deputy Headteacher or School Manager before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a child or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the child or adult must report the incident immediately to the first available member of staff, the Headteacher or Deputy Headteacher. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSP will refer details to social care or the police.

5. Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables children to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health and Computing Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for children to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Children are taught to recognise the creative, collaborative,

cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)

- understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, password, email address) and the importance of maintaining maximum privacy online

- thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- understanding the permanency of all online postings and conversations, including those previously posted on any form of social media

- understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images

- understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- how the law can help protect against online risks and abuse.

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with children.

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (Appendix C).

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the Online Safety Policy effectively and help keep children safe. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked to read and discuss with each child the Acceptable Use Agreement upon entry to the School. This should be reviewed by the parent/carer on a bi-annual basis. This will take place at the beginning of each Key Stage and half way through Key Stage 2. A summary of key parent/carer responsibilities will also be provided and is available in Appendix L. The Acceptable Use Agreement explains the school's expectations and child and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to children and staff are minimised.

The Headteacher/DSP undertakes termly checks using the software Senso (via IntermIT) to monitor staff, Governor, child, volunteer and visitor internet usage. Any inappropriate content will be flagged and investigated.

All breaches of this policy must be reported and all reported incidents must be logged via CPOMS. All staff have the individual responsibility to ensure that incidents are correctly recorded, acted upon and reported.

The school supports children and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

9. Appendices of the Online Safety Policy

Appendix A – Online Safety Acceptable Use Agreement – Staff, Governors, student

teachers

Appendix B – Online Safety Acceptable Use Agreement – Peripatetic teachers/coaches and supply teachers

Appendix C – Online Safety Acceptable Use Agreement – Requirements for visitors, volunteers and parent/carer helpers

Appendix D – Online Safety Acceptable Use Agreement – Guidance on the process for responding to cyberbullying incidents

Appendix E – Online Safety Acceptable Use Agreement – Guidance for staff on preventing and responding to negative comments on social media

Appendix F – EYFS Acceptable Use Agreement

Appendix G – KS1 Acceptable Use Agreement

Appendix H – KS2 Acceptable Use Agreement

Appendix I – Parent/Carer Acceptable Use Agreement

Broxbourne CE Primary School
Early Years & Extended Schools

Appendix A

Online Safety Lead - Paul Miller

Designated Safeguarding Person (DSP) – Paul Miller

Online Safety Acceptable Use Agreement – Staff, Governors & student teachers

You must read this agreement in conjunction with the online safety policy and the Data Protection policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Headteacher or Deputy Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the Headteacher or Deputy Headteacher and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy). I understand that Broxbourne CE Primary School uses SENSO monitoring software to monitor my online activity.

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Headteacher or Deputy Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to children and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or children on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or children.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or children.

Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

School Social Media Accounts

All communications must be approved by the Headteacher, Deputy Headteacher or School Manager before they are posted;

only posts that show the school in a positive light will be agreed;

all communications on our Twitter account must be clear and transparent;

children's names and photographs of children should not be used;

only school devices may be used to post communications;

once a post has been agreed, staff are required to block comments before posting;

any inappropriate/abusive comments must be reported immediately to the Headteacher, Deputy Headteacher or School Manager;

requests from children to follow our Twitter account must not be accepted;

parents must be notified if a request to follow our account is made from a child;

staff are not permitted to respond to comments made on the site;

parents must use official channels (e.g. email) to converse with school staff.

Passwords

I understand that there is no occasion when a password should be shared with a child or anyone who is not a staff member, unless a visitor such as a PTA member or a supply teacher needs access to a school computer.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or governing body
- personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, children or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of children.

I will not access secure school information from personal devices unless a closed, monitorable system has been set up by the school.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the Headteacher.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, children or parents/carers) to the Headteacher, DSP or Deputy Headteacher or Deputy DSP.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of children. I will also check the appropriateness of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Headteacher.

Video Conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school owned device should be used when running video conferences where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment and/or my responsibilities as an employee/governor.

Signature …….…….…… Date ……

Full Name ……..... (printed)

Job title ……

Appendix B

Online Safety Acceptable Use Agreement - Peripatetic Teachers/Coaches/ Supply Teachers and Students

Broxbourne CE Primary School

Online Safety Lead - Paul Miller

Designated Safeguarding Person (DSP) – Paul Miller

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy). I understand that Broxbourne CE Primary School uses SENSO monitoring software to monitor my online activity.

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Headteacher, Deputy Headteacher or School Business Manager.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to the Headteacher or School Business Manager and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to children and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Headteacher.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or children on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or children.

In my professional role in the school, I will never engage in 1-1 exchanges with children or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or children. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

School Social Media Accounts

All communications must be approved by the Headteacher, Deputy Headteacher or School Manager before they are posted;

only posts that show the school in a positive light will be agreed;

all communications on our Twitter account must be clear and transparent;

children's names and photographs of children should not be used;

only school devices may be used to post communications;

once a post has been agreed, staff are required to block comments before posting;

any inappropriate/abusive comments must be reported immediately to the Headteacher, Deputy Headteacher or School Manager;

requests from children to follow our Twitter account must not be accepted;

parents must be notified if a request to follow our account is made from a child;

staff are not permitted to respond to comments made on the site;

parents must use official channels (e.g. email) to converse with school staff.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a child or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.

- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, children or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, child's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the Headteacher/DSP, or a young person's or parent/carer's own device.

Use of Email

I will use my professional or formal student email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of children. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support child learning. Children can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the Headteacher.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, children or parents/carers) which I believe may be inappropriate or concerning in any way to the Headteacher or DSP.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of children.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Headteacher

Video Conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership DPO and DSP. A school-owned device should be used when running conferences, where possible.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ……..…….……..… Date ……

Full Name ……..... (Please use block capitals)

Job Title/Role ……..……..……

Broxbourne CE Primary School

Early Years & Extended Schools

Appendix C

Requirements for visitors, volunteers and parent/carer helpers

(Working directly with children or otherwise)

Online Safety Lead - Paul Miller

Designated Safeguarding Person (DSP) – Paul Miller

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the Headteacher and/or DSP

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.

- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.

- I will not give out my personal details such as mobile phone number, email address, and social media account details to children and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the DSP or Headteacher is informed before I leave the school.

- I understand my visit to the school may give me access to privileged information about children, staff, school systems and plans. Such information should never be shared online, including on social media sites.

- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.

- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of children. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

- I understand that Broxbourne CE Primary School uses SENSO monitoring software to monitor my online activity.

Social networking

I understand where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or children.

In my school role, I will never engage in 1-1 exchanges with children or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or children. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Visitors, volunteers and parent/carer helpers are not permitted to contribute to or comment on the school's social media accounts.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ……..…….……..… Date ……

Full Name ……..... (Please use block capitals)

Job Title/Role ……..……..……

Appendix D

Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Children should report to a member of staff (e.g. class teacher, Headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix E

Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy guide - summary of key parent/carer responsibilities, clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a child are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

  Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

- The meeting must:

  - draw attention to the seriousness and impact of the actions/postings;
  - ask for the offending remarks to be removed;
  - explore the complainant's grievance;
  - agree next steps;
  - clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need

to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;

- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Broxbourne CE Primary School

Early Years & Extended Schools

EYFS Acceptable Use of Technology Agreement / eSafety Rules

- I will ask an adult before I use any technology resources in the classroom e.g. metal detectors, mobile phones etc.
- I will make sure that when I am using IT, I am kind and friendly.
- In EY1, I will only go onto a pre-loaded IT activity.
- In EY2, I will choose an IT activity from our class book and ask a teacher to set it up for me.
- I will treat our IT resources with respect and put them away properly.

Broxbourne CE Primary School

Early Years & Extended Schools

Key Stage 1

Online Safety Acceptable Use Agreement

- I will only use IT in school for school purposes with the permission of a teacher/adult in the school.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my IT passwords. I understand I am responsible for any usage which takes place through any of my accounts. I will report any unusual activity to my Class Teacher.
- I will only edit/open/delete my own files including those found in shared drives.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my screen and tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not upload or add any images, videos, sounds or text to any shared to personal drive which could upset a member of the school community.
- I know that my use of IT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.
- I will not wear a smart watch at school which has photo taking options on it or enables receiving messages.
- I will not sign up to online services until I am old enough.
- I will not request to follow the school's Twitter account. I understand that my parents will be notified if I request to do so.

Broxbourne CE Primary School

Early Years & Extended Schools

Key Stage 2

Online Safety Acceptable Use Agreement

- I will only use IT in school for school purposes with the permission of a teacher/adult in the school.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my IT passwords. I understand I am responsible for any usage which takes place through any of my accounts. I will report any unusual activity to my Class Teacher.
- I will only edit/open/delete my own files including those found in shared drives.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my screen and tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not upload or add any images, videos, sounds or text to any shared to personal drive which could upset a member of the school community.
- I know that my use of IT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.
- I will not wear a smart watch at school which has photo taking options on it or enables receiving messages.
- I will not sign up to online services until I am old enough.
- When I am in Year 5 or 6, if I bring my mobile phone to school, I understand it must be switched off and remain in my bag for the duration of the school day.
- I will not request to follow the school's Twitter account. I understand that my parents will be notified if I request to do so.

Broxbourne CE Primary School

Early Years & Extended Schools

Parent / Carer Acceptable Use Agreement

Dear Parent / Carer

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you and your child need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with the class teacher.

Parent / Carer Responsibilities

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for children, relevant to their EYFS or their Key Stage.

- If internet research is set for homework, teachers may suggest specific sites. It is not advisable to allow your child to use Google as this may return undesirable search results. It is advised that parents check these sites first and supervise this work.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than your own child. When a parent/carer is on school premises, their phone/s must be switched off or on silent mode and out of sight.

- Parents/carers should not assume that children can bring technological devices to school and should always check the school policy.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.). The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable, block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school have chosen to set up a Twitter account and may add other school social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school's name or logo in any form. Parents may choose to follow the school Twitter account; however, children are not permitted to do so. Parents will be notified if their child requests to follow the school Twitter account.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, children and parents/carers.

Please return the signed sections of the Acceptable Use Agreements, relevant to your child/ren's Key Stage

or EYFS. If you have any concerns or would like some explanation, please contact your child's class teacher.

The school provides online safety information for parents/carers, through the website, in newsletters and at events.

Please see the full online safety policy in the policies section on the school website.

Broxbourne CE Primary School

Early Years & Extended Schools

Acceptable Use Agreement

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the promise I have made and my responsibilities.

Child's name……..…… Year ……

Child's signature……..

I/We have read and understand my responsibilities within the Acceptable Use Agreement:

Parent(s)/Carer(s) name(s)…….

Parent/carer signature……..……..

Date ……..…