Bramcote Hills Primary School

Online Safety Policy

Acceptable Use Policy

Written & Updated: May 2022
Updated: July 2023
Updated: November 2023

Key personnel

Designated safeguarding lead (DSL)	Peter Taylor Headteacher head@bramcotehills.notts.sch.uk
Computing Lead	Jonathan Minta jonathanminta@bramcotehills.notts.sch.uk
Technical support	ATOM support@atomit.co.uk
Date of which this policy was reviewed and by whom	Thursday 12th May 2022 Jonathan Minta

Date of next review and by whom	Monday 17th July 2023 BHPS Governors

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governors who oversees online safety are Mr Atkinson and Mr Stanley.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, The ICT Manager (Atom) / Computer Lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 2 contains a self-audit for staff on online safety training needs)

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Ensuring that the school engages in appropriate filtering and monitoring activity on school devices (on and off site) and on the school Wifi. All areas of concern should be followed up and all activity summarised and reported to the governing body. At the time of writing this is being done by ATOM and senior DSLs receive a daily report.

This list is not intended to be exhaustive.

3.4 The ICT manager (Atom)

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.1 The Rationale of using Project Evolve as a teaching tool for online safety

Project Evolve

At Bramcote Hills we have adopted the Project Evolve toolkit which is based on UKCIS framework "Education for a Connected World" (EFACW) that covers knowledge, skills, behaviours and attitudes across eight strands of our online lives from early years right through to the end of Key Stage 2 and beyond. These outcomes or competencies are mapped to age and progressive. The statements within the Project Evolve website are used as a guide by teaching staff as to the areas to discuss with pupils as they develop their use of online technology.

The 8 strands as detailed in the UKCIS framework "Education for a Connected World" (EFACW) are as follows:

- Self-Image and Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health- Well-being and Lifestyle
- Privacy and Security
- Copyright and Ownership

Pupils at Bramcote Hills Primary School will have the opportunity to develop their knowledge and build upon their understanding of each of the eight strands as they progress from year group to year group on their educational journey.

Self-Image and Identity
Pupils will have the opportunity to explore the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes. This strand also identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

Online Relationships
Pupils will have the opportunity to explore how technology shapes communication styles and identifies strategies for positive relationships in online communities. Pupils will have the opportunity to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Online Reputation
Pupils will have the opportunity to explore the concept of reputation and how others may use online information to make judgements. It also offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.

Online Bullying
Pupils will explore bullying and other online aggression and how technology impacts those issues. Pupils will also explore strategies for effective reporting and intervention and consider how bullying and other aggressive behaviour relates to legislation.

Managing Online Information
Pupils will explore how online information is found, viewed and interpreted. Pupils will focus on strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. Pupils will also explore how online threats can pose risks to our physical safety as well as online safety. Pupils will also be shown learning relevant to ethical publishing.

Health- Well-being and Lifestyle
Pupils will explore the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. Pupils will also focus on understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

Privacy and Security
Pupils will explore how personal information can be used, stored, processed and shared. Pupils will focus on behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

Copyright and Ownership
Pupils will explore the concept of ownership of online content. They will explore strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 1). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendix 1.

8. Pupils Using Mobile Devices in Schools

The school strongly discourages children bringing their mobile phone into school. However, we acknowledge that there may be a small number of occasions where parents prefer their child to carry a mobile phone to and from school. Before a child brings their phone into school, a request must be made from a parent/carer using the following MS Forms: https://forms.office.com/r/ac50ppXJjJ After parents have completed the MS Forms, they should email the school to inform the year 6 lead.

Upon receipt of this, a member of school staff will contact the parent to approve or deny the request. If the request is approved, the child will be permitted to bring their mobile phone into school. When arriving at school, children must turn off their phone and present it to their class teacher, who will

place it out of sight within the classroom. At the end of the day, children should ask to have their phone returned to them from their teacher.

The same approach is to be taken with smart watches that can access the internet and/or take photos.

Children **must not** use their mobile phone for any purpose whilst on school grounds (within the green, exterior fence). Whilst outside of school, children should continue to comply with the school's acceptable use policy – see below.

The school cannot be held accountable for any loss or damage to a child's mobile phone.

The following paragraph is an extract from the school's medicines administration policy.

In recent years there has been significant developments in the use of mobile phones and wearable technology to enable individuals to self-manage their own health needs. These developments are especially relevant to the management of diabetes and further information can be found here. Educational settings wherever possible should allow children and young people to use electronic devices such as mobile phones and smart watches to self-manage their health needs. Parents / carers must put in writing a request for the use of electronic devices. The child's / young person's Intimate Care and Health Plan should include details of the use of electronic devices for health self-management. Educational settings may need to revise their ICT policies to reflect this guidance.' (Section C, 6 page 14)

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software (Atom)
- Keeping operating systems up to date by always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Atom.

Staff are also aware that their activity on school devices both in and out of school and their use of their own devices on the school Wifi will be filtered and monitored by Atom in accordance with KCSiE 23.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the computing lead. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Bramcote Hills Primary School

Pupil, Parent/Carer and Staff Acceptable Use Agreement
Updated: May 2022

Make the Future Better for All

We all have access to the internet, either at home or at school, and it is an important part of our everyday life. We can use the internet to help us learn, for entertainment and to improve communication. However, we all need to follow the rules below to help us stay safe on the internet and to be fair to others – at school and at home.

Pupils

- I will only use the school computers for schoolwork or homework – unless given permission by a member of staff.
- I will only log in with my own username and password.
- I will keep usernames and passwords, at school and at home, private and will not share them with others, except for a caring/responsible adult.
- I will not use other people's login details or access their accounts.
- If I use school websites at home (e.g. Times Table Rockstars), I will use these appropriately.
- I will only edit and delete my own files and will not look at or change other people's files without their permission.
- I will only use the internet under the supervision or guidance of an adult.
- I will not bring files, CDs or memory sticks into school without permission and understand that, if I do, these will be virus checked before being used. I will make sure that my memory stick only contains items of schoolwork or homework.
- I will not use any chat or social network sites at school, unless supervised by an adult as part of a learning opportunity.
- I am aware that some websites and social network sites have age restrictions, and I should avoid using these sites at school and at home.
- I will only email people I know, or my parent/carer or teacher has allowed me to.
- Any messages I send via email or age-appropriate social networking sites will be polite, friendly and sensible.
- I will only use my own accounts and I will never pretend to be someone else when using age-appropriate social media sites.
- I will not open an attachment or download a file unless I know and trust the person who has sent it.
- I will not share any personal details over the internet such as my name, address, telephone number, name of school or photographs of myself or others.
- I will not arrange to meet anyone I have met over the internet and understand that I must tell a responsible adult if anybody suggests this.
- I will not try to befriend any members of school staff on the internet.
- If I receive a message I do not like or see something that I think might be wrong, makes me unhappy or uncomfortable, I will tell my parent/carer or my teacher.

- I understand that the school can check my files and the internet sites that I have visited at school at any time.
- When I am using the internet to find information, I will check that the information is accurate as I understand the work of others may not always be truthful.
- I understand that the school's devices and Wifi are filtered and monitored. This is for my own safety. I understand that any areas of concern will be investigated and action may be taken.

Parent/Carers

- Parents/carers may take photographs of their own child during school events (e.g. sports day, concerts and musical events). Any photographs which contain other children must not be uploaded to social media sites or shared in any way. This rule will be re-evaluated on a regular basis and parents/carers will be informed if it changes.
- Parent/Carers must switch off / mute their mobile phone when in school.
- Parent/Carers must not take photos of children in school except in relation to concerts or performances as indicated above.
- Some chat and social networking sites have age restrictions e.g. Facebook (minimum age 13). If you allow your child to use these sites, please be aware that any problems that may arise can upset children. School may attempt to assist with a problem up to a certain level but ultimately cannot be responsible for content that is written away from the school site. In extreme cases, the school may pass on the information to the police or appropriate authority.
- We suggest that parents using the internet at home with children adopt a similar set of safety rules to those agreed at school for consistency.
- Parents/carers should be aware that inappropriate use of the internet in connection with school matters could result in legal action being taken. Inappropriate use could include making negative comments about staff, pupils or school policies. The school has a complaints procedure to deal with parental concerns.
  Parents/Carers understand that the school's devices and WiFi are filtered and monitored. This is to help ensure the safety of pupils and staff. I understand that any areas of concern will be investigated and action may be taken.

Staff

The purpose of internet use in school is to assist pupils to achieve increasingly high standards, to support the professional work of staff and enhance the school's management and communication. Following these rules will help us protect ourselves against any risks.

- I will make sure that pupils are supervised as closely as possible when using the internet or are given clear instructions regarding what to do in independent study.
- I will only use school equipment to take photographs or videos for school purposes.
- I will not take or store any photos of children on my personal devices.
- I will only save work to a memory stick that has been encrypted.
- I will ensure that I am aware of each child's level of photograph consent when publishing photographs.
- I will not publish a child's full name alongside a photograph/video of them.
- I will use my school email address for work purposes and not my personal email address.

- I will ensure that any confidential information that is passed on electronically is password protected (email) or sent on an encrypted device.
- I will not share my school passwords with other staff.
- I will take full responsibility for the safety and security of any equipment loaned to me by the school and will not use it for inappropriate purposes. It will not be used by members of my family or my friends.
- I will respect the license restrictions of any software that I use.
- I understand that I should not befriend a pupil, parent, future parent or ex-pupil of school age on a social networking site. If I do, I understand that I might not have the backing of the school should an allegation be made.
- I will endeavour to check the suitability of online resources before using them and I am aware that these can change at short notice.
- I will not post information or photographs about myself or school-related matters on social networking sites that I would not want employers, colleagues, parents or pupils to see or that might compromise my professionalism.
- I will only use personal email or social networking sites at school when children are not present and when on break times.
- I will not browse, download or send to colleagues any material which could be considered offensive.
- I will not use a computer or other device in school that does not have up-to-date anti-virus software.
- I will report any accidental access to, or receipt of, any inappropriate materials or filtering breach to the Head Teacher.
- I will embed the school's online safety curriculum into my teaching.
- I understand that the school's devices and Wifi are filtered and monitored. This is to help ensure the safety and wellbeing of pupils and staff. for my own safety. I understand that any areas of concern will be investigated and action may be taken inline with safeguarding and disciplinary procedures.

All pupils at BHPS have access to the school's computer facilities including the internet as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign below to show that the rules have been understood and accepted. We ask that you discuss the agreement with your child to ensure that he/she fully understands the rules.

Pupil's Name: _____

Parent/Carer Name: _____

As the parent or legal guardian of the above pupil, I have read and understood the attached school acceptable use agreement and now grant permission for my son/daughter to use the internet, school network and other ICT facilities at school.

I accept that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that they will take every reasonable precaution to keep pupils safe and to prevent pupils accessing inappropriate materials.

I understand that the school has an educationally filtered service, restricted access email and provides age-appropriate teaching around internet use and online safety issues.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

I agree not to post or share images taken in school on social networking sites.

Parent Signature: _____

Date: _____

Appendix 2: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

APPENDIX 3

Useful websites

Gives details of age-appropriate social media websites	https://www.internetmatters.org/resources/social-media-networks-made-for-kids/
The most recent Education for a Connected World document	https://www.gov.uk/government/publications/education-for-a-connected-world
The UK Council for Internet Safety	https://www.gov.uk/government/organisations/uk-council-for-internet-safety