Broad Oak Primary School

www.broadoak.lancs.sch.uk

POLICY

Online Safety Policy

Learning to live, loving to learn.
At Broad Oak we nurture today's minds for tomorrow's challenges. Working together we ensure every child has the potential to shine.

Together we Challenge Aspire Nurture

CONTENTS

Introduction

The Online safety Policy is part of the School Development Plan and will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security and Child Protection.

Our Online Safety Policy has been written by the Computing Co-ordinator. It has been agreed by the senior leadership team and approved by Governors. It will be reviewed annually.

Technology is commonplace and its effective use is an essential life skill. Unmediated access to a range of resources brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. A policy is required to help ensure acceptable use; where the safety of pupils and staff is safe guarded. Online Safety depends on staff, school governors, advisors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and associated communication technologies. The Broad Oak Acceptable Use Policy intends to address all aspects of responsible internet use by both adult and child users and states clearly what the expectations and responsibilities of all users are. As communication technologies develop, we anticipate reviewing and where necessary amending our policies accordingly for the benefit of all users.

Governors, staff, community groups, and any visitors requesting access to our network should sign a copy of the Acceptable Use Policy and return it to the Head Teacher. Children will have their responsibilities explained and made clear to them and the Acceptable Use statements will be clearly displayed in all areas of school. The children will understand that technology is for learning and the understanding that the rules are there to protect them and be adhered to. Through clear Online Safety discussions in each class throughout the year, children will be reminded of the consequences of the misuse of technology. We will encourage the children to understand that Online Safety is a priority at home as well as school and that if they follow the basic rules of responsible use then the Internet is a very positive tool crossing all boundaries of race, religion gender and class.

The school Onlinonline safety Coordinator is the Computing Subject Leader: Rebecca Benton.
The responsible member of the Governing Body is: S Naylor Chair of Governors

The Designated Senior Leader is: Kelly Dytham

1. **Scope of the Policy**

This policy applies to all members of Broad Oak Primary School community who have access to and are users of school ICT systems, both in and out of the school.

The school will deal with any e safety incidents detailed within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/ carers of incidents of inappropriate online safety behaviour that takes place out of school.

At Broad Oak we will take all steps to ensure that Internet and e-mail access is appropriate and safe. In common with other media such as magazines, books and video, some material available via the Internet and e-mail is unsuitable for pupils. The school will take all reasonable precautions to ensure that such material is inaccessible. This is facilitated by the school taking their Internet access through BT Lancashire Services, which provides secure, filtered internet access for schools. However, due to the international scale and linked nature of information available via the Internet and e-mail, it is not possible to guarantee that particular types of material will never appear on a computer.

However neither the school nor the Lancashire Authority can accept liability for the material accessed, or any consequences thereof.

2. Roles and Responsibilities

I. Governors:

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy

II. Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Head teacher and another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

III. Mrs R Seat is responsible for the content of the school website.
Any online safety concerns that parents have can be discussed with the Computing subject leader whose contact details are on the schools website.

IV. Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Head teacher / subject leader for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level.

V. Child Protection / Safeguarding Designated Person; should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online bullying

VI. Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy

3. Policy Statements

I. Education – pupils
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and at Broad Oak it is provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PHSE / other lessons.
- All children receive at least one focused online safety lesson each half-term
- Key online safety messages are reinforced as part of a planned programme of assemblies or themed weeks.
- Children are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

II. Education – parents / carers
Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site. Monthly newsletter is sent out to parents.
- Parents evenings / sessions
- High profile events / campaigns eg: Safer Internet Day
- Reference to relevant web sites.

4. Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2) will be provided with a username and secure password by the subject leader who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (R Seat) must also be available to the Head teacher and subject leader and kept in a secure place.
- The school technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users using Netsweeper.

5. The management of e-mail in school:

- E-mail is regarded as an essential means of communication and school will monitor its use and content.
- Communication using e-mail is for appropriate educational use and not for private or personal messages.
- The language and content of e-mails should be of an appropriate level expected of any written work and should ensure that the good name of the school is maintained.
- The forwarding of chain letters and anonymous letters is banned.
- Staff and pupils should be aware that all e-mail on the school system is regarded as public and as such will be monitored.
- Pupils will only be given e-mail access for educational activities through a secure account.
- E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content.
- Staff and pupils should be made aware of the potential for virus infection through the sending or receiving of files attached to e-mails.
- The school e-mail system is primarily for educational use. Occasional and reasonable personal use is permitted provided that it does not interfere with the performance of school duties.

6. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. The images will be deleted from the camera/iPad as soon as the children have finished using them in their work.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.
- Looked after children must not be photographed without consultation and permission of the social worker. All staff must work with the DSL when organising any events regarding a looked after child.

7. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.
When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to the nominated person – the headteacher - in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

- Whole class / group email addresses may be used by the pupils.
- Staff mobile phones: staff may make and receive calls, but only in the confines of the upstairs or office areas. Private mobiles must not be used in view of the pupils.
- Pupils mobile phones will not be allowed in classrooms and, if necessary, will be kept in the school office.

8. Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the computing subject leader and head teacher to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

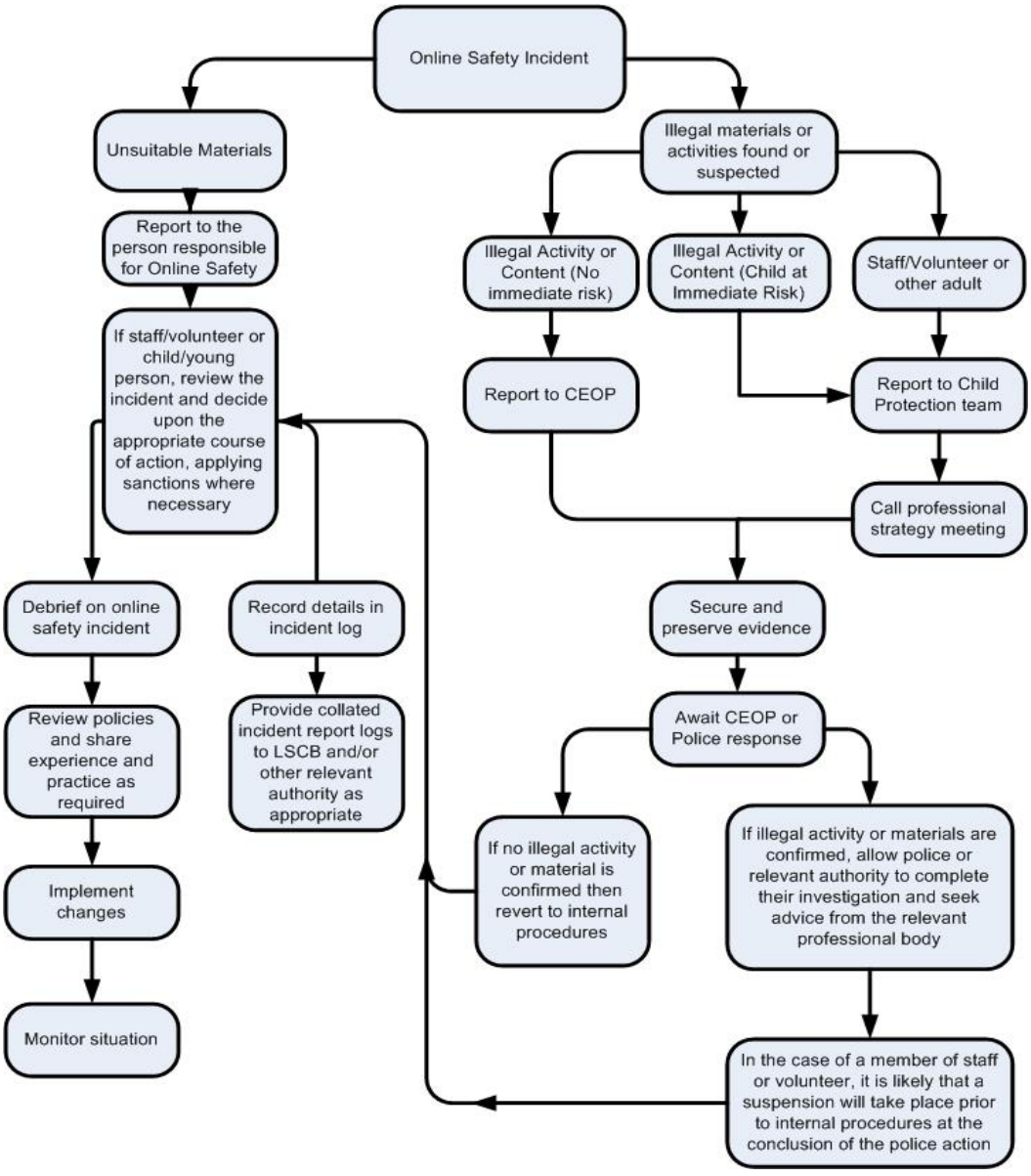
9. Publishing material on the school's website:

- The school will maintain editorial responsibility for any school initiated website to ensure that content is accurate and quality of presentation is maintained
- The school will maintain the integrity of the school website by ensuring that responsibility for uploading material is never handed over to pupils and that passwords are protected.
- The website will comply with the school's guidelines for publications
- The point of contact on the website will be the school address, e-mail and telephone number. Home information or individuals' e-mail addresses will not be published.

- School should obtain permission from parents via the use of the contact information from each September for the use of pupils' photographs. Group photographs should not have a name list attached. Identities of pupils must be protected at all times and parents may be consulted about publishing work from pupils.

10. Unsuitable / inappropriate activities

If there is any suspicion that the website(s) concerned may contain unsuitable images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



11. School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling incidents will be given to a senior member of staff (head teacher)
- Pupils and parents will be informed of the procedure
- Parents and pupils will need to work in partnership with staff to resolve any issues arising
- The facts of the case will need to be established, for instance to ascertain whether the issue has arisen through home Internet and e-mail use or through contacts outside school
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies
- Sanctions for irresponsible use will be linked to the school's Behaviour Policy and will consist of the following actions depending on circumstances:

    - Discussion with Class teacher/Head Teacher
    - Letter home /discussion to inform parent or carer
    - Further consequences such as withdrawal of Internet and e-mail privileges depending on circumstances

12. Data Protection

Personal data will be recorded, processed, transferred and made available according

to the General Data Protection Regulation (GDPR - 2018)

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

Individuals have a right to obtain confirmation regarding whether their data is being processed (along with a right of access to their personal data) by making a Subject Access Request (SAR). SARs need to be responded to within 1 month of the request, as per GDPR stipulations.

It is the school’s responsibility to ensure all relevant information is provided to the individual in compliance with GDPR requirements.

13. Development / Monitoring / Review of this Policy

This online safety policy has been developed and agreed by the:

- Computing Subject Leader
- Head teacher and Senior Leadership Team
- Staff – including Teachers, Support Staff, Technical staff
- Governors

14.Schedule for Development / Monitoring / Review

This Online safety policy was approved by the Governing Body on:	
The implementation of this Online safety policy will be monitored by the:	Subject Leader Senior Leadership Team
Monitoring will take place at regular intervals:	Once a year
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once a year
The Online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	April 23
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Computing Subject Leader Headteacher

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of:
  - students / pupils
  - parents / carers
  - staff

Broad Oak Primary School

Policy reviews

We are aware of the need to review our school's policies regularly so that we can take account of: new initiatives, changes in the curriculum, developments in technology etc.

This policy was reviewed in: April 22

To be reviewed: April 2023 (Sooner if required)

Acceptable Use Policy for Key Stage 2 Pupils

- I will only use the school Computing equipment for purposes I have agreed with a member of staff.
- I will keep my password private.
- I will not interfere with anyone else's passwords, logins, settings or files on the computer.
- I will always seek permission before downloading material from the internet or using material I have brought into school because I understand the risks from virus infections.
- I understand that I should only publish material on the internet that is my own work.
- I know I need permission to take someone's photograph or video them.
- Any messages I post on the Learning Platform or send in an email will be polite and responsible.
- I will not send or forward messages, or create material, which is deliberately intended to cause upset to other people.
- I will inform an adult if I see or receive any unpleasant material or messages.
- I know I must take care about giving away my personal information and making contact with people I do not know using the internet.
- I understand that the school may check my use of ICT and contact my parent/carer if they are concerned about my Online safety.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may apply even if the activity was done outside of school.

Pupil name .....

Signed .....

Acceptable Use Policy for Key Stage 1 Pupils

- I will ask before I use the school Computing equipment at break times or after school.
- I will keep my password private (Year 1 & 2 only).
- I will look after all the school Computing equipment and use it properly.
- I will always ask before downloading from the internet or using material I have brought into school because I understand the risks from virus infections.
- I will only put my own work on the internet, with permission from a teacher.
- I will only take a photograph or video of someone if they say it is alright.
- All of the messages I send will be polite.
- I will not send messages which upset other people.
- I will tell an adult if I see anything which upsets me.
- I will not give away my personal information or talk to people I do not know using the internet.
- I understand that the school may check my use of ICT and talk to my parent or carer if they are worried about my Online safety.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a period of time, even if it was done outside school.

Pupil name .....

Signed.....