NEW BARN SCHOOL

New Barn School

E-SAFETY POLICY

ACADEMIC YEAR 2021 - 2022

Document Type	Policy	**Version Number**	4.0
Policy Owner	Head teacher	**Last Review Date**	September 2021
Date First Issued	September 2018	**Next Review Date**	September 2022

CONTENTS **Page**

1.0 INTRODUCTION

E-Safety encompasses Internet technologies and electronic communications such as mobile phones.

This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy will operate in conjunction with other school policies including those for ICT, behaviour, anti-bullying, PSHE and child protection.

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

- Websites
- Learning Platforms (MLE) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Implementation: It is the responsibility of line managers to ensure that staff members are aware of and understand this policy and any subsequent revisions.

Compliance: This policy complies with all relevant regulations and other legislation as detailed in the *Compliance with Regulations & Legislation Statement*.

2.0 TEACHING & LEARNING

Why is internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is a part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services, professional associations and between colleagues;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to tools of direct communication, including video conferencing and email;
- Exchange of curriculum and administration data with Hampshire Authority and DCSF; and
- Access to learning whenever and wherever convenient

How can Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the ICT subject leader/System Administrators.
- Pupils must follow the procedure for reporting unsuitable Internet content which is shared with all pupils by their class teacher.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect Copyright when using Internet material in their own work.

How will our ICT system security be maintained?

- New Barn contracts the approved Acorn Education and Care Company 'Eclarity and the school ICT systems is reviewed regularly with regard to security.
- Virus protection is installed and updated regularly.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The ICT Subject Leader/ Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.
- The use of user logins and passwords to access the school network are enforced.

How will e-mail be managed?

- Pupils must tell a teacher immediately if they receive offensive e-mail.
- The instance will be recorded by the System Administrator and appropriate sanctions applied.

- Pupils are taught not reveal personal details of or those of others, or arrange to meet anyone in e-mail or other electronic communication, in line with e-safety guidelines.
- Excessive social e-mail use can interfere with learning and may be restricted.
- The forwarding of chain messages is not permitted.

How should Web site content be managed?

- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head teacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school.
- The Website should comply with the school's guidelines for publications.
- The copyright of all material must be held by Acorn Education and Care or be attributed to the owner where permission to reproduce has been obtained. Safeguarding our students is paramount.

Can pupils' images or work be published?

- Images which include pupils will be selected carefully and only those children whose written parental permission has been sought will be identifiable.
- Written permission is given by parents or carers when children start with the school. This data is held on the school's network.
- Pupils' full names will not be used on the Website when associated with photographs, or in any way which may be to the detriment of pupils.
- Pupil photographs will immediately be removed from the school upon request from parents, or other appropriate request.

How will social networking and personal publishing be managed?

- The school will block access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.

- Teachers' official blogs or Facebook should be password protected and never run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.

- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

How will filtering be managed?

- The school will adhere to the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Subject Leader/ Designated e-Safety Coordinator.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any material that the school believes is illegal must be referred to the IWF or CEOP (please see references given later).

- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of pupils.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.

Content

- Recorded material shall be stored securely.

- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third-party intellectual property rights.

- New Barn recognises video is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- If it is a non-school site, it is important to check that they are delivering material that is appropriate for the class.

- Test links should be set up prior to the session. Teachers are responsible for ensuring the content is suitable for all pupils to access.

How can emerging Internet uses be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time.

- The school investigates wireless, infra-red and Bluetooth communication technologies and has decided a policy against mobile phone use in school public areas.

- Young People are not provided with internet code for the school.
- Mobile phones are handed into reception.
- The sending of abusive or inappropriate text messages is forbidden. To ensure this, students may not use the school network to send text messages nor may they use instant messaging.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to The General Data Protection Regulations 2018.

3.0 POLICY DECISIONS

How will Internet access be authorised?

- All staff and pupils will initially be granted access to the school's electronic communications.
- Parents/carers and stakeholders will be informed that pupils will be provided with supervised Internet access.
- Pupils will not be allowed to use computers with Internet unless they are directly supervised by a member of staff.

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Hillcrest Care can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimize risks will be reviewed regularly.
- The Head teacher will ensure that the e-safety policy is implemented and compliance with the policy monitored.

How will e-safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse must be referred to the Head teacher.
- Pupils and parents/carers/stakeholders will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Sanctions available include:

- interview/counselling by senior member of staff/class teacher/teaching assistants;
- informing parents or carers;
- removal of Internet or computer access for a period, which could prevent access to school work held on the system.

How is the Internet used across the community?

The school will liaise with local organisations to establish a common approach to E-safety.

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Cyberbullying

Cyberbullying can be defined as:

"The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF2007.

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects.

A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.

Promoting a culture of confident users will support innovation and safety. There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006: every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils.

How will Cyberbullying be managed?

These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents gives head teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff. Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

There are clear procedures in place to support anyone in the school community affected by bullying.

There are clear procedures in place to investigate incidents or allegations of Cyberbullying. All incidents of cyberbullying reported to the school will be recorded. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence. The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers and all stakeholders of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.
- A phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation. Mobile phones and personal devices will not be used during lessons or formal school time. They are handed in to staff on arrival to school.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Cyberbullying and sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. Serious incidents may be managed in line with our Safeguarding Policy and child protection procedures.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Pupils Use of Personal Devices

- Students do not use personal phones during the school day. Students hand in all devices upon arrival to school.

- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.

- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy then disciplinary action may be taken.

The Designated Safeguarding Leads (DSL) are responsible for investigating all e-safety issues that may pose a safeguarding risk; e-safety issues are almost always safeguarding issues and may include serious concerns such as sexting, grooming and cyberbullying. It is the principal task of the DSL to see that all members of New Barn School community are properly educated to cope with the dangers that may arise from internet use.

COMMUNICATION OF POLICY

How will the policy be introduced to pupils?

- Rules for Internet access will be posted on or near all computer systems with Internet access.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use both at school and home.
- Internet safety guidelines will be prominently linked from the home page of the school's intranet and Internet sites.
- Pupils will be informed that Internet use will be monitored.
- Pupils receive an e-safety lesson at the start of each academic year.
- Instruction in responsible and safe use should precede Internet access.
- E-safety days are scheduled in to the school year.

How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff should only operate monitoring procedures on instruction from the Leadership Team.
- Staff training in safe and responsible Internet use, and on the school e-Safety
- Policy will be provided as required.

4.0 RELATED SAFEGUARDING POLICIES

- Anti-bullying
- Behaviour
- Child Protection
- Confidentiality
- CRB Disclosure Checks
- Disciplinary Procedure
- Equal Opportunities
- Extended School Activities
- Health and Safety
- Parent/carer Involvement
- Peer on peer abuse
- School Personnel Code of Conduct
- School Trips
- PSHE/RSE
- Visitors & Contractors
- Whistle Blowing

5.0 RAISING AWARENESS OF THIS POLICY

We will raise awareness of this policy via:

- the School Handbook/Prospectus;
- the school website;
- meetings with parent/carers such as introductory, transition, parent/carer-teacher consultations, etc.;
- school events;
- meetings with school personnel;
- communications with home such as end of term reports, etc.;
- information displays in the school.

6.0 EQUALITY IMPACT ASSESSMENT

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school.

7.0 MONITORING THE EFFECTIVENESS OF THIS POLICY

Annually (or when the need arises) the effectiveness of this policy will be reviewed by the coordinator, the Head teacher and the nominated governor and the necessary recommendations for improvement will be made.

	Local Authority Designated Teams	West Berkshire

Important Telephone Numbers		01635 519982
		Hampshire
		01962 876355
	Thames Valley Police	01865 841148