Baytree School

Online Safety Policy

Mandatory/Non-Mandatory		Mandatory
Model Policy		
Annual/Bi-Annual		Annual
Date Ratified by FGB		13th November 2024
Signed (Chair of Governing Board)		
Next Review Due		November 2025

'It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.'

The breadth of issues clarified within online safety are considerable and can be categorised into four areas of risk:

- ***Content*** *– being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism*

- ***Contact*** *– being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes*
- ***Conduct*** *– personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and*
- ***Commerce*** *– risks such as online gambling, inappropriate advertising, phishing and or financial scams.*

Keeping Children Safe in Education 2023 – page 35

Aim

- Have robust processes and procedures in place to ensure the online safety of learners, staff, volunteers, visitors 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.
- Establish clear mechanisms to identify, intervene and escalate an incident where appropriate.

Responsibilities

The Governing Board has responsibility for:

- Monitoring and ensuring the implementation of this policy at Baytree School
- Coordinating regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead

The Headteacher/Deputy headteacher are responsible for:

- Ensuring that all staff understand this policy
- Monitoring and ensuring the implementation of this policy consistently throughout Baytree School

The designated safeguarding lead is responsible for:

- Ensuring that all staff understand the policy and that it is being implemented consistently throughout the school
- Work alongside the Headteacher and other staff, as necessary, to address any online safety concerns, issues or incidents
- Ensuring that any online safety incidents are logged using CPOM's and dealt with in line with this policy
- Ensure that any online safety concerns of cyber-bullying are logged using CPOM's and dealt with appropriately in line with the school behaviour policy
- Updating and delivering regular staff training on online safety
- Liaise with other agencies and/or external services
- Providing regular feedback and reports on online safety to the Governing Board

All staff, visitors and contractors are responsible for:

- Understanding and implementing this policy consistently throughout Baytree School
- Agreeing and adhering to the acceptable use policy and ensuring that learners follow the school's guidelines on acceptable use
- Working with the designated safeguarding lead to ensure that any online safety incidents are reported, recorded 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's behaviour policy

This is not an exhaustive list.

Online safety is paramount to the safeguarding of all children and young people in the digital world. It is about learning to understand and use technologies in a positive way, and about supporting children and young people to develop safe online behaviours (both in and out of school).

DFE Online Safety Guidance – updated January 2023

Baytree School Online Safety Curriculum (embedded through the PSHE/RSHE curriculum) will support and enable learners to understand and gain greater depth of knowledge to know:

- what positive, healthy and respectful online relationships look like
- the effects of their online actions on others
- how to recognise and display respectful behaviour online

Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their learners' lives.

This includes:

- how to use technology safely, responsibly, respectfully and securely
- where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Online safety encompasses not only internet technologies, but also other means of electronic communications, such as mobile phones, games consoles and wireless technologies.
The Internet is an essential element in 21st century life for education, business and social interaction. It is developing constantly and therefore, as a school, we must reflect this to ensure learners develop the necessary skills to keep themselves safe online. The Internet is part of the statutory curriculum and an entitlement for learners as part of their learning experience. It is used in this school to raise educational standards, promote learner achievement and is a necessary tool for staff to support their professional work. The Internet also enhances the school's management information and business administration systems.

In common with other media such as magazines, books and videos, some material available via the Internet is unsuitable for learners. The school has a duty of care and will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

Neither the school nor North Somerset Council can accept liability for the material accessed, or any consequences of Internet access.

The Benefits to the School
Benefits of using the Internet in education include:

· A vast range of free and subscription educational resources to enhance the learning experience of learners;
· Access to world-wide educational resources;
· Educational and cultural exchanges between learners world-wide;
· Access to experts in many fields for learners and staff;
· Staff professional development, through access to national developments, educational materials and good curriculum practice;
· Communication with support services, professional associations and colleagues;
· Exchange of curriculum and administration data with the LA and DfE;
· Mentoring of learners and provision of support for them and teachers.

Internet Access
Internet access will enhance learning. Learners will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use, in line with DFE - Teaching online safety in school Guidance June 2019.

· School Internet access will be designed expressly for learner use and will include filtering appropriate to the age of the learners.
· Staff should guide learners in online activities that will support the learning outcomes planned for the learners' age and maturity.
· Internet access will be planned to enrich and extend learning activities.
· Learners will be educated in the effective use of the Internet in research, including learning the skills to locate, retrieve and evaluate knowledge.
· All staff must read and sign the staff "Acceptable Use Policy" before using any school ICT resources.

All staff must read and sign the Baytree School social media expectations document annually.

All visitors/volunteers must read and sign the visitors "Acceptable Use Policy" before using any school ICT resources.

Management of E-mail
· Staff and learners may only use approved e-mail accounts on the school system (Office 365). This is administered by office admin where new accounts can be set up or old ones deleted.
· Learners must have adult supervision whilst using e-mail and be taught principles of how to keep themselves safe online.
· Learners must immediately tell a teacher if they receive offensive e-mail.
· Learners must not reveal personal details of themselves or others in an e-mail communication, such as address or telephone number, or arrange to meet anyone without specific permission.
· E-mail sent by learners to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Internet Content
· Learners will be taught to question online information before accepting it as true.
· The school will ensure that use of Internet-derived materials by staff and learners complies with copyright law.

· Learners will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.
· Learners will be encouraged to tell a member of staff immediately if they encounter any material that makes them feel uncomfortable.

The School Website
· The point of contact on the Website should be the school office address, e-mail and telephone number. Staff or learners' personal information will not be published.
· Website photographs that include learners will be selected carefully and will not enable individual learners to be identified. Photographs will only be published with parental permission
· Learners' full names will not be used anywhere on the website, particularly in association with photographs.
· The Headteacher will delegate editorial responsibility to office admin to ensure that content is accurate and quality of presentation is maintained.

Internet Dangers and Risk Assessment
Baytree School will take all reasonable precautions to ensure that users access only appropriate material.
An e-safety co-ordinator has been appointed to oversee Internet dangers, risk assessment and matters arising from Internet use. However, neither the school nor North Somerset Council can accept liability for the material accessed, or any consequences of Internet access.
E-safety meetings are held three times a year to review incidents and safe practice at Baytree.
· Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
· The school will audit ICT provision to establish whether the online safety policy is adequate and that its implementation is effective.

Social Networking and Personal Publishing
· The school, via South West Grid for Learning (SWGfL), will block access to social networking sites.
· Newsgroups will be blocked unless a specific use is approved.
· Pupils and parents will be advised that the use of social network sites outside school is inappropriate for primary aged pupils.
· Learners will be advised never to give out personal details of any kind which may identify them or their location, or place personal photos online, or arrange to meet someone without specific permission from parents/carers.
Baytree School will use the Baytree School Twitter and Facebook accounts to celebrate learners' successes, engage with other professionals, and advertise relevant events to parents/professionals and link with other schools. The Headteacher will delegate editorial responsibility to office admin to ensure that content is accurate and that quality of presentation is maintained. Photographs of learners will only be published on Twitter with parental permission.

Cyberbullying
'Cyberbullying is bullying that takes place online. Unlike bullying in the real world, online bullying can follow the child wherever they go, via social networks, gaming and mobile phones' (NSPCC website) and can include any of the following:

- Sending threatening or abusive messages
- Creating and sharing embarrassing images or videos
- Trolling – the sending of menacing or upsetting messages on social networks, chat rooms and online games
- Excluding children from online games, activities or friendships groups
- Shaming someone online
- Setting up hate sites or groups about a particular child

- Encouraging young people to self-harm
- Voting for/against someone in an abusive poll
- Creating a fake account, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- Sending explicit messages known as sexting
- Pressuring children into sending images or engaging in sexual conversations.

It is not a specific criminal offence but there are laws that apply to associated behaviour, such as the Protection from Harassment Act 1997 or the Malicious Communications Act 1988. It is important that children and young people keep any evidence of cyberbullying and that they realise that the police will be able to trace the originator of any messages.

Many young people and adults find using the internet and mobile phones 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 and a once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.
Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents reported will be recorded and investigated.

Filtering
· The school will work in partnership with the LA, DfE and the Internet Service Provider (South West Grid for Learning, SWGfL) to ensure systems to protect pupils are reviewed and improved.
· If staff or learners discover an unsuitable site, the URL (address) and content must be reported to the Deputy Headteacher and the Internet Service Provider informed in order for the site to be blocked.

Emerging Technologies
· Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.
· Mobile phones must not be bought into school unless the Headteacher/Deputy Headteacher has given permission. The sending of abusive or inappropriate text messages is forbidden.
· The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
· The e-safety co-ordinator will ensure that the e-safety policy is implemented and compliance with the policy monitored (all staff will be required to sign a form declaring they have understood the e-safety policy and its procedures).

Information System Security
· School ICT systems capacity and security will be reviewed regularly by 2IT Systems who regularly monitor the network.
· Virus protection will be updated regularly (Sophos, purchased annually).
· Security strategies will be discussed with North Somerset Council and the IT Company which supports the curriculum.
· Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

The Policy and Pupils
Online safety will be introduced to the learners through lessons and constant reinforcement and an Safer

Internet day
· Online safety rules will be posted in all rooms where computers are used and discussed with pupils at the start of each year. Implementation of the online safety rules will be checked regularly by the e-safety co-ordinator. Pupils will take part in Safer Internet day annually (as appropriate).
· Pupils will be informed, as appropriate, that Internet use will be monitored and access will be withdrawn if the facility is abused
· The school will keep a record of all learners who are granted Internet access. The record will be kept up-to-date, for instance if a pupil's access is withdrawn or if pupils leave or join the school.
· Instruction in responsible and safe use will precede Internet access.
· Learners work can only be published on the website with the permission of the learners and parents.

The Policy and Staff
It is important that all staff are confident using the Internet in their work. The school Internet policy will only be effective if all staff subscribe to its values and methods.
· All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource.
· The school will keep a record of all staff who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves.
· All staff including teachers, supply staff, teaching assistants and support staff, will be provided with the online safety Policy, and its importance explained.
· Staff should be aware that Internet and e-mail traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
· Staff development in safe and responsible Internet use will be provided as required.
· Any breaches of the Acceptable Use Policy will be referred directly to the Headteacher.
· Staff should be aware that if using social networking sites their profiles should be private and that the school, pupils or staff must not be discussed. It is also not acceptable to have pupils (or past pupils) as online contacts. It is suggested that Parents/Carers are not online contacts. If they are, staff should conduct themselves professionally, profiles should be private and school matters should not be discussed or commented on.
Any concerns or breaches should be reported to The Headteacher immediately.

ICT Security
The school ICT systems will be reviewed regularly with regard to security.
· Virus protection will be installed and updated regularly by 2IT Ltd (IT Support)
· Security strategies will be discussed with the LA/SWGfL.
· Photographs of learners should only be taken using school equipment. In exceptional circumstances, with specific authorisation, personal cameras/phones can be used and images immediately transferred to the school network and then deleted from the camera memory. All images must be stored in the staff area on the network, not on curriculum computers or on school laptops unless the equipment has encryption software for reports/pupil evidence.
· Administrative data sent over the Internet will be encrypted or otherwise secured.
· Use of portable media such as memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
· 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 2IT manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

Complaints

· Responsibility for handling Internet misuse incidents will be taken by the online safety co-ordinator.
· Any complaint about staff misuse must be referred to the Headteacher.
· Complaints of a child protection nature must be dealt with in accordance with school child protection procedures which adhere to the North Somerset Safeguarding Children Board requirements.
· Pupils and parents will be informed of the complaints procedure.
· Parents and pupils will need to work in partnership with staff to resolve issues.
· There may be occasions when discussions will be held with the Police to establish procedures for handling potentially illegal issues.
· Sanctions available for pupil misuse include:
- interview/counselling by e-safety co-ordinator;
- informing parents or carers;
- removal of Internet or computer access for a period of time.

Internet and the community
· Where possible the school will liaise with local organisations to establish a common approach to e-safety.

Parental Support
· Parents' attention will be drawn to the School e-safety policy in newsletters, the school prospectus and on the school website.
· Internet issues will be handled sensitively to inform parents without causing undue alarm.
· A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

For further information please refer to the most up to date guidance/policies/documents listed below:

- Acceptable Use Policy
- Baytree School – staff code of conduct
- Acceptable Use Agreement for Internet, Email, School ICT Networking and Equip
- Our ICT Rules
- Rules for Acceptable Use of ICT and the Internet
- Pupil Rules for Acceptable Use of ICT and The Internet
- Acceptable Use Agreement – Adult Visitors
- School's Social Media/Networking Policy
- Baytree Schools social media expectations document
- Personal Data Policy
- Campus Joint Mobile Phone Policy
- DFE - Teaching online safety in school Guidance supporting schools to teach pupils how to stay safe online when studying new and existing subjects – June 2019
- Online Safety Act 2023 **www.legislation.gov.uk/ukpga/2023/50/enacted**

Policy Review

Reviewed by FGB: 18th November 2020 Next review due: November 2021	Reviewed by FGB: 17th November 2021 Next review due: November 2022	Reviewed by FGB: 16th November 2022 Next review due: November 2023	Reviewed by FGB: 16th November 2023 Next review due: November 2024	Reviewed by FGB: 13th November 2024 Next review due: November 2025	