



COMPUTING

Online Safety and Usage Policy

Updated: Autumn 2023

Old Basford School's Online Policy has been updated in line with the 'Keeping Children Safe in Education 2023' document.

OBS Vision Statement

Intent

At Old Basford School we want our pupils to be confident and responsible users of technology. Technology is everywhere and it plays a pivotal part in the lives of our pupils and will also play a vital role in their futures. We ensure that our online safety teaching addresses the four areas of risk as mentioned in the 'Keeping Children Safe in Education 2023' document, including: content, contact, conduct and commerce.

We believe that 'A high quality computing education equips our pupils to use computational thinking and creativity to understand and change the world.' We hope that our children use technology creatively, our broad curriculum reflects this encompassing: core skills, digital literacy, computer science, data handling and online safety. Online safety is of high priority throughout the school. **We believe it is essential that children are safeguarded from potentially harmful and inappropriate online material and because of this, we take a whole school approach to online safety to protect and educate our pupils and staff in their use of technology, intervening, and escalating any concerns where appropriate.**

At OBS we want our children to understand that when using technology there is always a choice. We also believe it is important that children know who they can turn to for support with online issues and that they can have safe and honest conversations about their online activity within their classrooms.

By the end of KS2, we want our pupils to be fluent with a range of tools to best express their understanding and hope that they have the independence and confidence to choose the best tools to fulfil task and challenges set by teachers.

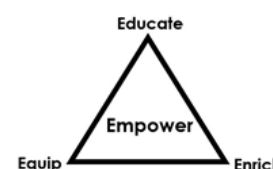
Our main intent is to deliver a curriculum that is centred around 'The 4 Es'.

We **educate** our children and give them the knowledge that they need.

We **equip** our children with the skills that they require.

We **enrich** our provision with opportunities that inspire and motivate.

When we have educated, equipped and enriched our children we will **empower** them with the desire to be life long learners.



Implement

We have created an OBS specific skills ladder for staff to follow to help embed and cover all elements of the computing curriculum **based on the 'Teach Computing' curriculum which is provide by the National Centre for Computing Excellence**. The knowledge/skills build year on year to deepen understanding and challenge learners. Some computing skills will be taught in explicit computing lessons either using technology or 'unplugged'. However, we have IPADS/Computer suite/laptop timetables which can be booked out for cross curricular lessons. An example of this could be a Year 4 history lessons where children show 'I can use search engines effectively' and can 'describe how some online information can be opinion'.

Impact

We encourage and support our children to use technology responsibly and creatively. Finding the right balance is key to an effective education and healthy lifestyle and we educate our children to know how to stay safe online and have an awareness of dangers they may face. Children have a growing 'toolkit' and as I school we are continuing to support children with both their digital literacy skills and their computer science skills. Progress of our computing curriculum is demonstrated through outcomes and the record of coverage in the process of achieving them.

The Curriculum

At Old Basford we use a whole school approach to online safety to protect and educate our pupils, students and staff in their use of technology. We understand that the breath of issues classified within online safety are considerable and ever evolving. We ensure that our online safety teaching addresses the four areas of risk including: content, contact, conduct and commerce.

The statutory curriculum we deliver aims to ensure that all pupils are responsible, competent, confident and creative uses of information and communication technology.

Key Stage 1 pupils will be taught to use technology safely and respectfully, keeping personal information private and to know that they need to go to an adult they trust for help and support when they have concerns about the content or contact on the internet of other online technologies (E.g. Mobile phones and tablets).

Pupils in **Key Stage 2** will be taught to use technology safely, respectfully and responsibly, to recognise acceptable and unacceptable behaviour and to identify a range of ways to report concerns about content and contact. They know they can go to any adult in school to report their concerns and worries.

We teach Online safety as part of both our computing curriculum and our PSHE curriculum. To ensure that online safety is ever present within school life, at the start of each computing lesson, children will briefly discuss/take part in an activity, known as an anchor task regarding different online safety issues. We use the 8 strands as recommended by the 'Education for a Connected World Framework' to ensure our e-safety teaching is up to date and current. There strands are as follows:

Self image and identity

Copyright and ownership

Online bullying

Online relationships

Online reputation

Privacy and security

Health, wellbeing and lifestyle

Managing information online.

Staff are encouraged to also use a reactive approach when planning these tasks to ensure they meet their children's ever changing needs. We also take part in the annual 'Internet Safety Day' as a whole school.

Internet Use in school

- Pupils will be supervised at all times whilst using the internet in school.
- Pupils will not be issued with individual e-mail accounts.
- Pupils are encouraged to tell a teacher immediately if they encounter any content that makes them feel uncomfortable. Staff should report any material that makes them uncomfortable or that is inappropriate to the computing co-ordinator or head teacher.
- Pupils are taught to ensure that their online behaviour is appropriate and to conduct themselves in an appropriate manner when both while on the school premises and while using technology outside of school.
- Pupils will be taught to be critically aware of the materials they read, including commerce, such as online gambling, inappropriate advertising and phishing and financial scams and will be shown how to validate information before accepting its accuracy (E.g. To avoid clicking on pop ups and links that are unsuitable)
- Pupils will be taught to acknowledge the source of information used and to comply to copyright when using Internet material in their own work.

Security

- Old Basford School has security protection procedures in place to safeguard our systems.
- The security of the whole system will be reviewed with regard to threats to security from Internet access and is managed by Nottingham City 'Schools IT'.
- Virus protection will be installed and updated regularly;

- Use of removable storage devices is allowed but they must have a Bitlocker code to ensure safety.
- Removable storage devices that have been provided by the school are for school use only.
- All school work should be kept on the server for safety as opposed to desktop and vulnerable removable storage devices. Work saved on desktops cannot be recovered, staff are responsible for keeping their work secure.
- Staff are strongly encouraged to use OneDrive to store documents they wish to access at home. They can also use this to back up important documents as these will be stored even if a laptop is damaged.
- Attachments on e-mail are used solely for school or education purposes.

Filtering

At Old Basford school our internet access is filtered. The filtering system has a number of categories blocked by default for staff and students. Individual websites are blocked or allowed based on their categorisation and also via their specific URL if entered manually. This ensures that our children and staff are not exposed to inappropriate or harmful content or are able to take part in harmful online contact with other users. Our IT Technician (Alan Bartlett) and the school Safeguarding team will conduct regular checks to ensure that the filtering methods are appropriate, effective and reasonable. School devices are also filtered off network (away from school) against the same policy that they would be under within school. All staff within school have a clear understanding of how to escalate concerns when identified. If staff or pupils discover unsuitable sites, the URL must be reported to the Computing coordinator, Head teacher or technician in order for our filtering systems to be updated.

For further information please see the 'Old Basford School Information and Filtering Policy' attached to this document.

Cyber Crime (information taken from The National Crime Agency) and Hacking

Skills in coding, gaming, computer programming, cyber security or anything IT-related are in high demand and there are many careers and opportunities available to anyone with an interest in these areas. However, as a school we need to have an awareness as these skills can also be used dangerously.

Cyber crime can be split into two broad categories:

- Cyber-dependent crimes (or 'pure' cyber crimes) are offences that can only be committed using a computer, computer networks or other forms of information communications technology (ICT). An example of a cyber-dependent crime is gaining unauthorised access into someone's computer network, this can also be called 'hacking'.
- Cyber-enabled crimes (such as fraud, the purchasing of illegal drugs and child sexual exploitation and abuse) can be conducted on or offline, but online may take place at unprecedented scale and speed.

Examples of cyber crime include:

- Unauthorised access – this involves gaining access into someone's computer network without their permission, and then taking control and/or taking information from other people's computers. Examples may include accessing the secure area on the school's computer network and looking for test paper answers or trying to change test scores.
- Making, supplying or obtaining malware (malicious software), viruses, spyware, botnets and Remote Access Trojans is illegal. These programmes allow criminals to get into other people's computers to carry out illegal activities. 'Pranking', by remotely accessing a friend's computer when they don't know you are doing it and messing around is still illegal.

Consequences of cyber crime

Cyber crime is a serious criminal offence under the Computer Misuse Act. The National Crime Agency and police take cyber crime extremely seriously and will make every effort to arrest and prosecute offenders.

Young people getting involved with cyber crime could face:

- A visit and warning from police or NCA officers
- Computers being seized and being prevented from accessing the internet
- A penalty or fine
- Being arrested
- Up to life in prison for the most serious offences

A permanent criminal record could affect education and future career prospects, as well as potential future overseas travel.

If you have any concerns about pupils or staff, you should report your concerns to parents. However if your concerns are serious, **you should contact the police via 101 or report it via Action Fraud.**

Managing information - Our Website content

- A designated member of the office team and head teacher will take overall responsibility and ensure that content is accurate and appropriate on the main school page.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained. All images used from search engines must not be copyrighted and staff should show children how to differentiate different types of copyright. Please use the advise from: <https://usingtechnologybetter.com/smarter-image-searching-five-ways/>
- Parents and carers are required to sign a permission letter for the publication of photographs on our website.
- Class teachers are aware of children who are not allowed their photographs online and take every care to ensure that these children are not present in group/class photographs.
- The work of pupils will only be published with their permission.
- Only the first name of pupils will be used with their permission.

Social Networking, social media and personal publishing

- Both pupils and staff will not be allowed to access public or unregulated chat rooms and social networks during school times.
- Our filter system will block access to social media and social networking sites.
- Staff should not request or respond to any communications with a child through social networking sites.
- During online safety assemblies, Computing and PSHE lessons, pupils will learn about their online conduct and will be advised not to give out personal details that could identify them or their location. Examples of this would include their full real name, address, the school they attend and phone numbers.
- Children in KS2 are aware of the THINK rules when using conducting themselves online and using social media apps outside of school.
- As a school, we also use the SMART rules to help the children stay safe online and to help safeguard our children from the 4Cs.

Mobile Phone Use

- Old Basford School has a clear policy on the use of mobile phones and children are not allowed to bring mobile phones in to school or on school site. If a child is found with a mobile phone it will be confiscated. A member of staff will ask the child to turn off their phone and it will be locked away and handed over to a responsible adult at the end of the day.
- Within assemblies and parent events, the use of mobile phones to record video footage is not allowed. If a parent/carer is spotted filming they will be asked to delete the footage in front of a staff member.
- Photographs by parents are allowed but they must not be shared on social media and this will be made clear at the beginning of every event.
- Staff are not to have their mobile phones out on desks and they should be put away in a safe place. They are not permitted to use their phone to photograph pupils. An exception to this is if a staff member is using their phone to provide music within a lesson or celebration (E.g. Dance teacher, Christmas party)

Cyber Bullying

At Old Basford we take any incidents of Bullying very seriously. Cyber bullying, along with all forms of bullying will not be tolerated in our school. We take every care to ensure that children understand that the internet is 'forever' and that they should conduct themselves appropriately online. Pupils are aware that bullying online is the same as bullying on the playground and that it won't be tolerated in our school.

- Pupils, staff and parents/carers are advised to keep a record of any bullying as evidence. Any incidents reported by parents or pupils will be logged on CPOMS.

Sanctions for those involved in Cyber Bullying include:

- Parents and carers will be informed of any incidents of cyber-bullying that have taken place outside of school and it will be their responsibility to discuss the incident with their child.

Training and Communication with staff and parents

- Rules for safe internet use will be posted in the computer room and the THINK and SMART motto is displayed in classrooms.

- The online safety policy will be available to parents via the school website. Communications are periodically sent to parents/carers throughout the academic year making them aware of the latest online issues, age ratings of games and website as well as information on current apps, games and platforms.
- Pupils will be informed that their internet use will be monitored.
- Assemblies about online safety and participation in the annual 'Safer Internet Day' which is organised nationally, will be done annually.
- The school website will contain a page advising children and parents of ways for their children to stay safe online and this will be updated regularly.
- **Staff received an online update as part of their Safe Guarding Training in September 2023, which was delivered by our Advanced Designated Safeguarding Lead.**
- All staff should closely monitor internet use within their classroom and in the computer suite.
- All staff need to report any Online Safety incidents to the computing coordinator or the head teacher.
- The Online safety policy has been updated in line with the 'Keeping Children Safe in Education 2023' document.

For further is the 'Old Basford School Information and Filtering Policy'

(This policy has been written by the Sarah Crosby, building on the Kent County Council SEGfL e-safety policy, advice from the national crime agency and government guidance. Updated Autumn 2023 by Julia Black)