Sir Alexander Fleming Primary School and Nursery
Online Safety (including Acceptable Use Policy)

Reviewed September 2026
Next Review September 2027

Introduction

Writing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for computing, bullying, behaviour and for child protection.

It has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed annually.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties: the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Why Internet use is important?

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. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. It is used to raise the standards of education, support professional work of staff and enhance the school's management. Primarily, it is used to promote pupil achievement.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include but are not limited to:

- The Internet – World Wide Web
- E-mail
- Instant messaging (e.g. Snapchat, Viber, Viber, Kik)
- Web based voice and video calling (e.g. Skype, facetime, Whatsapp, Omegle)
- Online chat rooms
- Online discussion forums
- Social networking sites and apps(e.g. Facebook, Whatsapp, Snapchat, TikTock)
- Blogs and Micro-blogs (e.g. Twitter).
- Gaming platforms (Discord/ PS4/PS5/ XBOX).
- Podcasting (radio / audio broadcasts downloaded to devices)
- Video broadcasting sites (e.g. YouTube)
- Music and video downloading (e.g. iTunes)

- Mobile phones with camera and video functionality
- Smart phones and watches with e-mail, messaging, apps and internet access

Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:
- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- Online Safety teaching is embedded into the school curriculum and schemes of work.

At the start of each computing lesson, pupils from KS1-KS2 receive an e-safety top-tip created by Education for a Connected World which teaches them the importance about staying safe online.

Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors and DSL's, aims to embed safe practices into the culture of the school.

Leadership team

The SMT ensures that the Policy is implemented across the school via the usual school monitoring procedures, including pupil voice.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the Online Safety Policy.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Staff ensure they are familiar with the school Online Safety policy, and ask for clarification where needed.

Class teachers ensure that pupils are aware of the Online Safety rules, introducing them at the beginning of each new school year and embedding them throughout the daily curriculum.

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with Online Safety issues, both at home and school. They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school and sign to say they accept these (please see Appendix 1)

Parents

Parents are given information about the school's Online Safety Policy at the admission interview. They are given copies of the pupil information and asked to support these rules with their children. As appropriate they are also sent Online Safety top tips via email, Facebook, Seesaw or on the school website every fortnight and an online safety newsletter every month. This is to address any current Online Safety topics that may be presenting themselves either in school or in the media. If an Online Safety issue has arisen with a particular group of children or year group, then communication is made with the relevant parents.

Internet Use & Management

Our service provider Roartech uses Senso monitoring software throughout the school and runs behind every software application. All users must read and sign the 'Acceptable Use Policy- Staff and Governors (Appendix 2) before using any school ICT resources. Senso is designed to protect users and will alert the Headteacher and Computing Lead of any potential breaches of the internet use policy which are then investigated and appropriate action is undertaken. (Screenshots are taken by the software at any instance of violation to allow easy tracking of the site/words used/user and computer involved).

The school 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 TAW can accept liability for the material accessed, or any consequences of Internet access.

Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. The school will ensure that the 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.

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. At Key stage 2, children accessing the internet are closely monitored.

Online Safety Education

Users are informed that network and Internet use is monitored and traced to the individual user. Online safety resources are used within school to teach children safe use of the internet. These resources a regularly updated, as the Internet and use of the Internet is constantly evolving. Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

Sir Alexander Fleming uses a range of materials including the CEOP website which includes a series of child-friendly lessons specifically catered to and differentiated for each Key Stage/Year group to teach them about all elements of Online safety. Integrated into this is an annual Safer Internet Day (February) dedicated to educating the children around the dangers surrounding internet/digital device use. This comprises of key stage assemblies (age-related) and is followed up by lessons to reinforce the messages. Other assemblies dedicated to E-safety are taught throughout the year, often by our pupil leadership team, the 'Digital Leaders'.

Teachers in Year 1-6 follow the Natterhub Online Safety Programme. We have chosen specific objectives and have mapped them into our long-term progression document, to ensure learning builds each year. The Natterhub lessons are designed to create discussion, and be engaging for the children. Children in EYFS follow a range of different materials, including Project Evolve, which has again been mapped as part of our long-term progression.

Pupil voice is often carried out to ensure that we remain up-to-date with the apps and ways in which our children use the Internet. The annual Bullying Survey, carried out in each year group, includes questions around all forms of bullying including that of the dangers of the internet. This ensures that we are clear of the pupils' understanding

around this area and in turn can take steps and measures to further educate where necessary. We also ensure that at least one question on the annual Parent survey is linked to E-safety so we can allow parent to have their say.

Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet for learning is now a part of the Computing Curriculum. We teach all our pupils how to find appropriate information on the Internet, and how to ensure as far as possible, that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials.
- Children are taught how to use search engines (such as Kiddle & Kidrex) and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

Teaching safe use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area: Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES
http://www.kidsmart.org.uk

The main aspects of this approach include the following five SMART tips:
- Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
- Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
- Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...
- Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...
- Tell your parent or carer if someone or something makes you feel uncomfortable or worried...

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

'It is essential that children are safeguarded from potentially harmful and inappropriate online material. We aim to protect and educate pupils, students, and staff in their use of

technology and establish mechanisms to identify, intervene in and escalate any concerns where appropriate.' Keeping Children Safe In Education 2022

Staff are aware of the breadth of issues classified within online safety and understand that it is consistently evolving. Staff receive regular CPD linked to E-safety via the E-safety Lead and follow the E-safety risk assessment daily. The risk assessment is categorised into four areas of risk (content, contact, conduct and commerce) . This risk assessment highlights those risks and the measures in place to reduce this risk. All staff in our setting have access to and are aware of this risk assessment.

Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home.

There is a selection of links to such resources available from on the school website, and in the shared pupil folders on the school network.

Unsuitable material

Despite the best efforts of the LA and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to a trusted adult at the time they occur, so that action can be taken.

The action will include:
1. Making a note of the website and any other websites linked to it.
2. Informing the technician (ICT administrator).
3. Logging the incident
4. Discussion with the pupil (and their parent) about the incident, and how to avoid similar experiences in future.

E-mail

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

Pupils are taught not to reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission. They are encouraged to immediately tell a teacher if they receive offensive e-mail. The forwarding of chain letters is not permitted.

Internet-enabled mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, watches, tablets, iPads and games consoles.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc. and how the data protection and privacy laws apply.

• Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school. If this is the case, mobile phones are taken to the school office and kept locked away until the end of the school day, where they are returned to the child. Consent via a parent/ carer must be completed in order for this to happen.

Published content and the school website

The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils' personal information is not published. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Written permission from parents or carers is obtained before photographs of pupils are published on the school website. A log is kept of children who we do not have permission to use their photographs and this log is updated regularly. Pupils' full names will not be used anywhere on the Web site or Blog if prior consent has not been obtained, particularly in association with photographs. Pupils work may be published on the website.

Social networking and personal publishing

The school will block/filter access to social networking sites. Pupils will be advised never to give out personal details of any kind that may identify them or their location whilst on the internet at school or home. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupil voice surveys often gives us the opportunity to find out what social networking sites the children are currently using so that staff can receive training about these sites if necessary.

Managing emerging technologies

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

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should be displayed in each classroom. Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Senso will capture any inappropriate searches and report instantly to the DSL.

Sanctions will include:

Unsuitable material: (e.g. online games, celebrity pictures, music downloads, sport websites etc)

• Initial warning from class teacher
• Banning from out of school hours Internet facilities

- Report to Headteacher
- Letter to parent/carer

Offensive material: (e.g. pornographic images, racist, sexist or hate website or images etc)
- Incident logged and reported to Head teacher
- Initial letter to parent/carer
- Removal of Internet privileges/username etc
- Meeting with Parent/Carer to re-sign Internet use agreement

Handling Online Safety complaints
Complaints of Internet misuse will be dealt with by a senior member of staff. 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.

Whilst it is the duty of the school to ensure that every child in our care is safe, the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, means it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences as a result of accessing the Internet.

Use of the Internet and ICT resources by school staff
The Internet
Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion. We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

Internet Availability
To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use. The school also provides a user account that gives further access to specific resources, online tools and email.

ICT Equipment and Resources
The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, digital cameras, sound recorders, control and data logging equipment and a range of professional and curriculum software.

Professional use
Staff are expected to model appropriate ICT and Internet use at all times (please see the Acceptable Use Policy – Staff and Governors- Appendix 3). This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support or CPD in using ICT as part of their professional practice can ask for support from the computing Coordinator or the school's Technology support (technician).

Personal use of the Internet and ICT resources

Some equipment (including laptops) is available for loan to staff, with permission from the Headteacher. The appropriate forms and agreements must be signed. However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use.

E-mail

We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, bulletin boards and forums, online chat and messaging

We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin board to share good practice and disseminate information and resources. The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

Social Networking

The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Conduct of Conduct expectations and agreements. As with discussion groups, staff are reminded that professional standards should apply to all postings and messages.

Data Protection and Copyright

The school has data protection policy in place – please see separate documentation for more details. Staff are aware of this policy, and how it relates to Internet and ICT use, in particular regarding pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

Click the link below to access the Acceptable User Agreements

Acceptable User Agreements

Appendix 2

Acceptable Use Agreement / Code of Conduct Staff, Governor and Visitor

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff areexpected t o sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Katy Tomlinson (online safety coordinator and DSL)

- Permission will be sought from students and parents before any photographs are published on a web site, blog or social media outlet.
- Images of children must not be published where it is possible to identify their names.
- Access must only be made via the authorised account and password, which must not be made available to any other person
- All Internet use should be appropriate to staff professional activity or student's education. Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- No hardware of software will be installed without the permission of the ICT coordinator.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden
- Copyright of materials and intellectual property rights must be respected
- All electronic communications with pupils/parents and staff must remain professional
- Own personal details, such as mobile phone number and personal email address must not be given out to pupils.
- Personal data must be kept secure and used appropriately, whether in school, taken off school premises or accessed remotely
- Any material that could be considered offensive, illegal or discriminatory must not be browsed, downloaded, uploaded or distributed.
- Internet access can be monitored and logged which can be made available, on request, to a line manager or Headteacher.
- Support of the school to online safety must be respected by not deliberately uploading or adding any images, video, sounds or text that could upset or offend any member of the school community.
- Online activity, both in school and outside, will not bring the professional role into disrepute.
- Support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of computing and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the School

Signature ……

Full Name ……(printed)

Job title …… Date……