# Sir Alexander Fleming Primary School and Nursery

## 'Belonging, Being, Becoming'

## Online Safety Policy

Updated: January 2023

Review Date: January 2024

### Our school values

SAFE – keep ourselves and others safe by making sensible choices within school, online and in the community.

RESPECT – have the social, emotional and nurturing skills to respect ourselves, our families and our communities.

PRIDE – be proud of what we all achieve by aspiring to work hard and become your 'best self'

BRAVERY – to overcome barriers by attempting difficult challenges by being resilient, independent and inquisitive.

SUCCESS – achieving high standards with a belief that with effort anything is achievable.

Writing and reviewing the online safety policy

The online safety policy relates to other policies including, ICT/Computing; Child Protection and Safeguarding; Acceptable Use and Social Media.

- The school's online safety co-ordinator is also the computing coordinator, as the roles overlap.

## Teaching and Learning

### Why internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.
- The school internet access is provided by Telford & Wrekin Council through a regional broadband contract, which includes 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.
- Pupils from all year groups will sign an acceptable user policy agreement.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

### Pupils will be taught how to evaluate internet content

- The school will seek to ensure that the use of internet derived materials by staff and by 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 how to report unpleasant internet content e.g. using the CEOP Report Abuse icon.
- For pupils whose parents lack economic resources, the school should build digital skills and resilience, acknowledging the lack of experience and internet at home.
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

## Managing internet Access

### Information system security

- School ICT systems security will be reviewed regularly by the ICT technician from T&W
- Service Provider (Roartech) filters information using Smoothwall (filtering system).
- WiFi access is password protected.
- Staff must use Senso to monitor and control what pupils are typing/accessing during use of computers/laptops to meet safeguarding responsibilities.
- InTune management solution is used to control what pupils are accessing on the school iPads maintains the safe use of technology.

### Managing filtering

- The school will work in partnership with T&W / Roartech to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator and/or the ICT Technician.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A log of any incidents on CPOMS will be used to identify patterns and behaviours of the pupils.

## E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to parent email (including Parent Mail texting service) communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as possibly suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

## Published content and the school web site

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The headteacher, and website administrators, will take overall editorial responsibility and ensure that content is accurate and appropriate.

## Publishing pupils' images and work

- Photographs that include pupils will be selected carefully based on context. The school will use photographs only when permission has been granted by the parent/carer and pupil
- Pupils' full names will be avoided on the website or learning platform including in any blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained as part of the admission process, before photographs of pupils are published on the school website or social media platform.

## Social networking and personal publishing on the school learning platform

- The school has a robust social media policy.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils and parents will be advised of the age restrictions set for the use of social network spaces outside school.

### Managing videoconferencing (if available)

- Videoconferencing will use the Telford and Wrekin network to ensure quality of service and security.
- All videoconferencing will be managed and supervised by the teacher
- Any videoconferencing will be conducted through Microsoft Teams or Google Meet using staff accounts

### Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons and formal school time unless permission has been granted by the Headteacher

### Protecting personal data

- Personal data will be processed in accordance with the requirements of GDPR legislation (or equivalent UK legislation)

## Policy Decisions

### Authorising internet access

- All staff, governors and visitors must read and sign the "Acceptable Internet and Computer Use Policy for Staff, Governors and Visitors" before using any school ICT resource. (Appendix 1)
- Pupils must sign an acceptable user policy agreement before accessing the school network. It is the responsibility of the class teacher to ensure this is adhered to.

### Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor T&W/Roartech can accept liability for the material accessed, or any consequences of internet access.
- The school will monitor ICT use to establish if the online safety policy is adequate and that the implementation of the online safety Policy is appropriate and effective.

### Handling online safety complaints

- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of internet misuse will be overseen by a senior member of staff.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet, and this is in line with the school's Behaviour Policy.

### Staff and the Online Safety Policy

- All staff will be advised of the school's Online Safety Policy and its importance explained.

- All staff will sign to acknowledge that they have read and understood the Online Safety Policy and agree to work within the stipulated guidelines.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be advised on the use of social media, both at work and in their personal situation through the Social Media policy.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school's Online Safety Policy in newsletters and on the school website and updates will be given.
- Parents are offered online safety training annually, with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

## 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 are expected to sign this policy and adhere at all times to its contents.

Any concerns or clarification should be discussed with Julie Lane (school online safety coordinator / 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 Online 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…………………….