FAIRLANDS PRIMARY SCHOOL

Pound Avenue
Stevenage
Hertfordshire
SG1 3JA

Headteacher: Mr Robert Staples BA (Hons)
Tel: (01438) 351053 E-mail: admin@fairlands.herts.sch.uk www.fairlands.herts.sch.uk

POLICY STATEMENT

ONLINE SAFETY

APPROVED BY GOVERNORS	September 2023
TO BE REVIEWED BY	September 2024

FAIRLANDS PRIMARY SCHOOL

ONLINE SAFETY POLICY

CONTENTS

1. INTRODUCTION

Fairlands Primary School recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and governors will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

2. RESPONSIBILITIES

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.

The named online safety co-ordinator in this school is Chris Holgate.

All breaches of this policy must be reported to the headteacher.

All breaches of this policy that may have put a child at risk must also be reported to the headteacher (DSL), or the deputy headteacher in each phase (DDSL).

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network and equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. SCOPE OF POLICY

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents:

- child protection
- code of conduct
- social media
- safeguarding
- data protection
- local health and safety
- home–school agreement
- behaviour management
- anti-bullying
- relationships, sex and health education.

4. POLICY AND PROCEDURE

The school seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account or Governor Hub for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors, and pupils should not open emails or attachments from suspect sources and should report their receipt to the headteacher.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e., cyberbullying).

Visiting online sites and downloading

Staff must preview sites, software, and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.

When working with pupils searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals, or comments that contain or relate to:

- indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e., images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- indecent images of vulnerable people over the age of 18 (i.e., images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- adult material that breaches the obscene publications act in the uk
- promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age, and marital status
- promoting hatred against any individual or group from the protected characteristics above
- promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- any material that may bring the school or any individual within it into disrepute e.g., promotion of violence, gambling, libel, and disrespect.

Users must not:

- reveal or publicise confidential or proprietary information
- intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- use the school's hardware and wi-fi facilities for running a private business
- intimidate, threaten or cause harm to others
- access or interfere in any way with other users' accounts
- use software or hardware that has been prohibited by the school

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the headteacher.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the headteacher. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g., for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child unless there is a pre-specified permission from the headteacher. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off.

Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage, or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Personal mobiles must never be used to access school emails and data. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the school office before they are brought into school.

Reporting incidents, abuse, and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive, or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL, the headteacher or deputy headteacher of the phase. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

5. CURRICULUM

Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety which enables pupils to become informed, safe, and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience, and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic, and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include:

- understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, im/email address) and the importance of maintaining maximum privacy online
- thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- understanding the permanency of all online postings and conversations
- understanding relevant legislation, including copyright, and the importance of respecting other people’s information, reputation, and images
- what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

6. STAFF AND GOVERNOR TRAINING

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers, and parent/carer helpers (Appendix E).

7. WORKING IN PARTNERSHIP WITH PARENTS/CARERS

We work closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F.

The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

8. RECORDS, MONITORING AND REVIEW

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported, and all reported incidents will be logged on CPOMS, using the online safety lozenge. Appendix I may be used if CPOMS is unavailable. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Appendix J gives a checklist of what information to include on CPOMS.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

9. APPENDICES OF THE ONLINE SAFETY POLICY

We have several appendices to this policy which are available on request from the school office:

A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)

B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers

C. Requirements for visitors, volunteers and parent/carer helpers working in the school (working directly with children or otherwise)

D. Online Safety Rules (Primary Pupils)

E. Online Safety Acceptable Use Agreements Secondary Pupils

F. Online safety policy guide - Summary of key parent/carer responsibilities

G. Guidance on the process for responding to cyberbullying incidents

H. Guidance for staff on preventing and responding to negative comments on social media

I. Online safety incident reporting form – *only used if CPOMS is unavailable*

J. Online safety incident record