The Fairisle Schools

Expect Success

Fairisle Junior School
E-Safety Policy

Introduction

This policy is designed to ensure safe internet use by pupils in our school, to help children keep safe online and to empower them to make sensible decisions and choices when using technology. The purpose of this policy is to ensure that all staff, children, parents, and governors understand and agree the school's approach to e-safety. The school’s e-safety policy should operate in conjunction with other policies including those for safeguarding, behaviour, anti-bullying and data protection. This policy and its implementation will be reviewed annually. Online safeguarding is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to online safety developments, whichever is sooner.

The Governing Body is accountable for ensuring that our school has effective policies and procedures for online safety. The safeguarding governor also takes responsibility for online safety, overseeing and evaluating how the school deals with any online safety incidents and keeping this policy under constant review.

Please refer to the school’s Child Protection & Safeguarding Policy for matters referring to cyber bullying, sexting and upskirting, as well as matters of child on child abuse.

Teaching and learning

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 children with quality internet access as part of their learning experience.
- Internet use is a part of the computing statutory curriculum and a necessary tool for staff and pupils.

Internet use enhances learning

- The school internet access provides filtering appropriate to the age of our pupils.
- Pupils are taught what internet use is acceptable and what is not and given clear objectives and non-negotiables for internet use.
- Internet access is planned to enrich and extend learning activities.
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation, as well as the laws regarding copyright and plagiarism.
- Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum.

Pupils are taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school computing leader, who will inform the Headteacher.
- The school ensures that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught how to report unpleasant internet content immediately to a member of staff through being Internet Legends, which teaches the children how to be Sharp, Alert, Secure, Kind and Brave online at a level that they understand.

Managing Internet Access

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not always possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access. The Headteacher & Computing leaders, supported by the computing technicians, will ensure that the e-safety policy is implemented and compliance with the policy monitored.

Information system security including Filtering

- School computing systems capacity and security are reviewed regularly.
- Virus protection is updated regularly.
- We purchase broadband from Virgin through Southampton City Council, with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed to access personal e-mails or chatrooms whilst in school.
- Pupils are taught that they must immediately tell a teacher if they receive an offensive email.
- Pupils are taught never to reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Staff to pupil and vice versa email communication must only take place via a school email address and is monitored.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the school's website is the school's address, email and telephone number. Staff or pupils' personal information are not published.
- The Headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils are selected carefully in line with parental wishes regarding individuals.
- Pupils' full names are not used anywhere on the website, particularly in association with photographs.
- Permission from parents or carers is obtained before photographs of pupils are published on the school website.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic devices e.g. iPads.
- In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use only. The Headteacher always reminds parents and carers not to upload images of other people's children to social networking sites.

Social networking, gaming and personal publishing

- The school blocks access to social networking sites and newsgroups except those that are part of an educational network. Children are advised not to use these at home.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents are advised that the use of social network spaces and certain online games used outside school may be inappropriate for primary aged pupils. Children are taught about PEGI ratings.
- Pupils are advised to use nick names and avatars when using social networking sites if they are accessing them outside of school.

Managing filtering

- The school works in partnership with the Local Authority and our service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover an unsuitable site, it must be reported to the school's computing leaders.
- The Business Manager and the computing leaders, alongside the computing technicians, ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies are examined for educational benefit and an educational/business case is completed before purchasing new technology for use in school.
- Children are not allowed mobile phones in school.
- Staff have access to a school phone where contact with pupils is required.

Protecting Personal Data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR). https://www.gov.uk/data-protection

Preventing Radicalisation

Online Safety

- The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school block inappropriate content, including extremist content.
- We also filter out social media, such as Facebook. Searches and web addresses are monitored and the computing technicians alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.
- Where staff, children or visitors find unblocked extremist content they must report it to a senior member of staff.
- The Acceptable Use of Technology Policy refers to preventing radicalisation and related extremist content. Staff are asked to sign this policy to confirm they have understood what is acceptable. What is acceptable for pupils is laid out clearly in each child's Planner.
- Pupils and staff know how to report internet content that is inappropriate or of concern through a whole school assembly at the beginning of every term
- Pupils are taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils are advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.

Policy Decisions

Authorising Internet access (See appendix)

- The Headteacher and Computing Leader maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the Acceptable Technology Use Policy before using any school resource.

- All staff who have a school laptop should only use it for school purposes and no member of their family or friends should have access to this computer.
- Staff who have permission to use remote access should only do so on an authorised computer and no data should be shared under any circumstances.
- Parents and pupils are expected to comply with the school's Responsible Technology/Internet Use Policy.

Handling E-Safety issues

- Complaints of Internet misuse are dealt with by the computing leaders in the first instance.
- 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 and reported to the Designated Safeguarding Lead.
- Pupils and parents are informed of the complaints procedure in the parent handbook.
- Sanctions within school include: – interview/counselling by class teacher / headteacher; – informing parents or carers; – removal of Internet or computer access for a period.
- When needed, we seek advice from the police on how to best deal with incidents. We also take account of Hampshire Constabulary's Safe4Me bulletins and updates on emerging local trends and issues around staying safe online.

Community use of the Internet

- The school is sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offers appropriate advice.

Communicating this Policy

Introducing the E-Safety policy to pupils and parents

- E-safety non-negotiables are discussed with the pupils at the start of each year.
- Non-Negotiables for computing and the use of technology are posted in all classrooms and computing suite as well as in pupils' planners. Pupils' planners also contain a page to explain 'Be Internet Legends'.
- Pupils and parents are informed that Internet use is monitored and parents are informed whenever inappropriate internet use is suspected.
- Advice on e-Safety is introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.
- The children receive e-safety lessons and are constantly reminded of online safety.
- The children receive lessons on protecting themselves from all forms of cyberbullying.
- We take part in Internet Safety Day annually and invite parents into lessons.
- Our school Twitter account (@FairisleJS) is used to share helpful advice for parents from National Online Safety.

Staff and the E-Safety policy

- All staff are given this policy and its importance explained.
- Staff should be aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' and carers' support

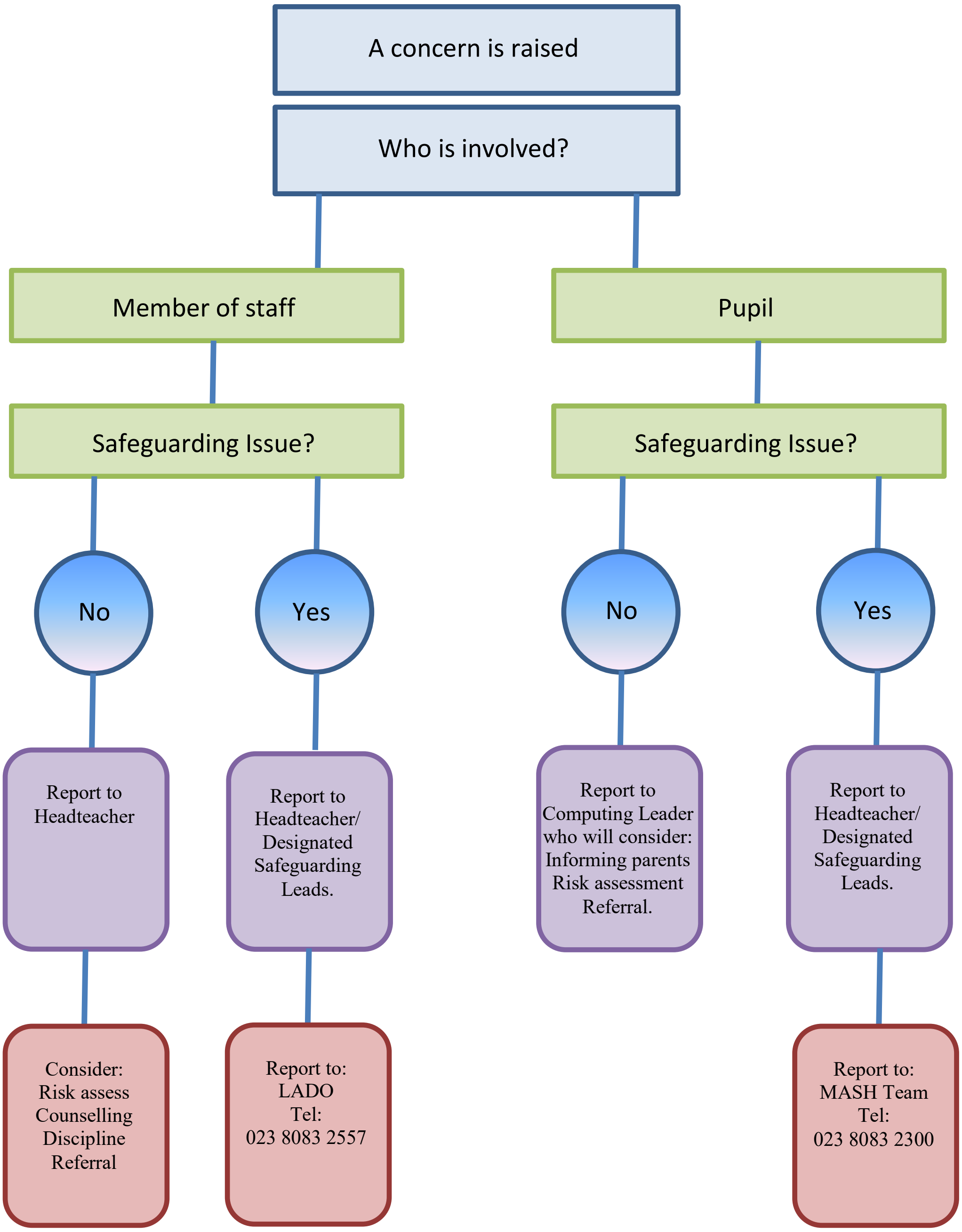
- Parents' and carers' attention is drawn to the School E-Safety Policy on the school website.

If using the internet at home:

- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils are made aware of how they can report abuse and who they should report abuse to.
- Pupils are taught the reasons why personal photos should not be posted on any social network space without considering how a photo could be used now or in the future.
- Pupils are advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils must only invite known friends and deny access to others.

Date of this Policy: **Spring 2024**
Policy to be Reviewed: **Spring 2025 (at the latest)**

Inappropriate Activity Flowchart



A concern is raised

Who is involved?

Member of staff

Safeguarding Issue?

No

Report to Headteacher

Consider:
Risk assess
Counselling
Discipline
Referral

Yes

Report to Headteacher/ Designated Safeguarding Leads.

Report to:
LADO
Tel:
023 8083 2557

Pupil

Safeguarding Issue?

No

Report to Computing Leader who will consider:
Informing parents
Risk assessment
Referral.

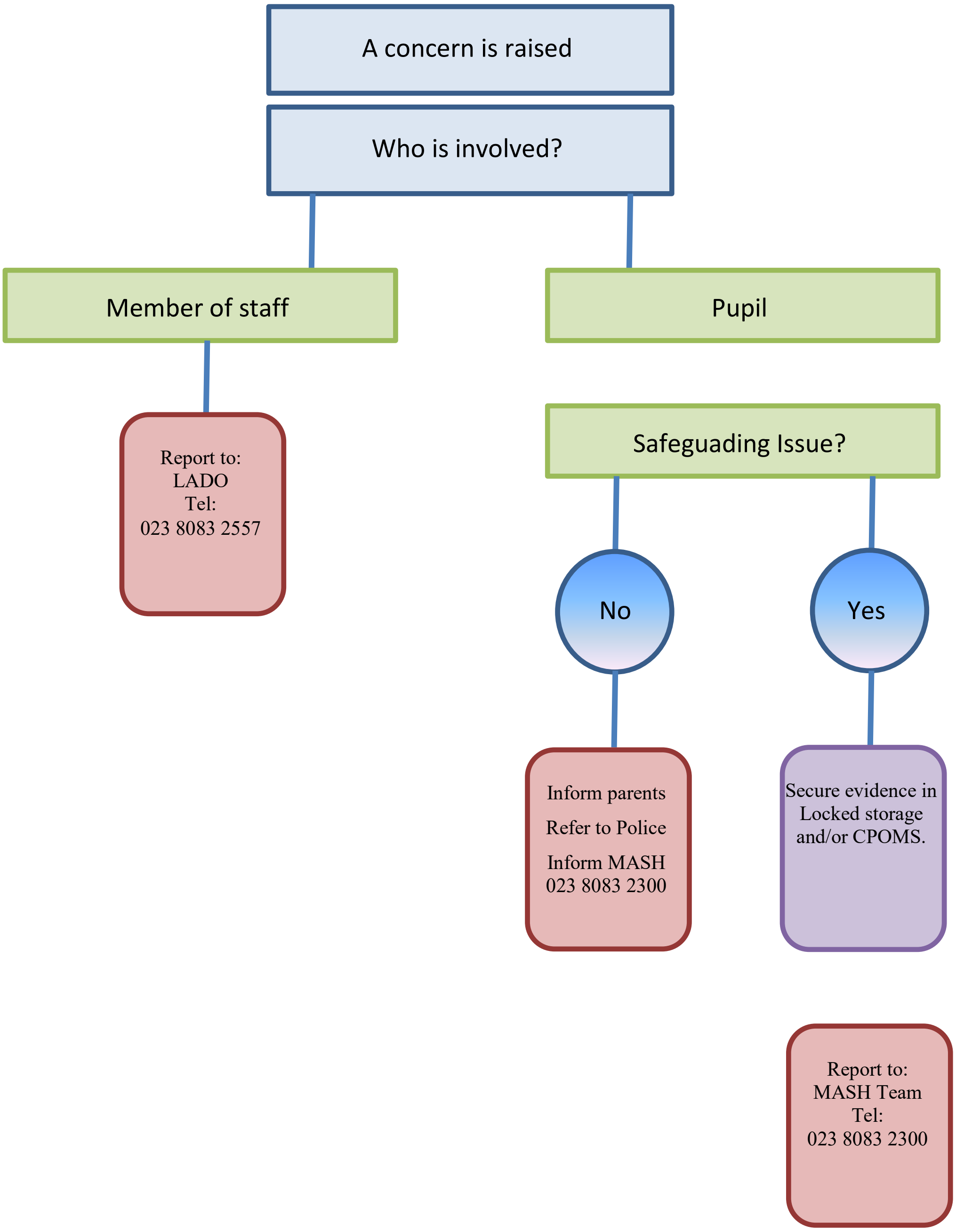
Yes

Report to Headteacher/ Designated Safeguarding Leads.

Report to:
MASH Team
Tel:
023 8083 2300

If you are in any doubt, consult the Headteacher, Designated Safeguarding Leads or Computing Leaders.

Illegal Activity Flowchart



A concern is raised

Who is involved?

Member of staff

Report to:
LADO
Tel:
023 8083 2557

Pupil

Safeguading Issue?

No

Inform parents

Refer to Police

Inform MASH
023 8083 2300

Yes

Secure evidence in
Locked storage
and/or CPOMS.

Report to:
MASH Team
Tel:
023 8083 2300

Never investigate.

Never show to others for your own assurance.

DO NOT let others handle evidence – Police only.