Southwater Junior Academy

E-Safety Policy

Links to Other Policies

The academy's e-safety policy will operate in conjunction with other policies including:

- Pupil Behaviour
- Anti-Bullying
- Child Protection
- PSHE Policy
- Curriculum
- Data Protection and Security

What is E-safety?

E-Safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, collaboration tools and personal publishing. E-safety concerns safeguarding children and young people in the digital worlds. It emphasises learning to understand and use new technologies in a positive way, about the risks and the benefits. E-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband including the effective management of filtering.

- A member of staff being responsible for the implementation and monitoring of this e-safety policy.

Introduction

The purpose of this policy is to:

- Through consultation with pupils establish the ground rules we have in Southwater Junior Academy for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our discipline and PSHCE policies.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence and to prevent radicalisation.
- Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.
- Demonstrate how to report inappropriate or illegal activity.

Teaching and learning

- 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.
- The academy internet access is designed specifically for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- 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' study of extremist and terrorist material for legitimate purposes is protected.
- Pupils understand the risks attached to accessing terrorist and extremist material online and understand the academy's duty and process in these areas.
- Pupils are safe from accessing extremist or terrorist materials whilst using academy servers.

Managing Internet Access

- The Academy ICT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly.

E-mail

- Pupils may only use approved e-mail accounts on the school system (London Grid for Learning (LGFL) - @southwaterja.co.uk email).
- Pupils must tell a teacher immediately if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on academy headed paper.

Academy website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- Photographs and videos that include pupils are carefully selected.
- Pupils' full names are not used anywhere on the Website or blog.
- Where photographs and videos of pupils are published on the school Website (including via Twitter and Facebook) parents or carers have given consent.

Social networking and personal publishing

- The academy blocks access to non-educational or age-related social networking sites
- Newsgroups are also blocked.
- Pupils are told never to give out personal details of any kind which may identify them.
- Pupils and parents are advised that the use of social network spaces outside of the academy is inappropriate for primary aged pupils.

Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported immediately to the Computing Subject Leaders, ICT technician or a member of the Senior Leadership Team.
- Senior staff ensures that regular checks are made to ensure that the filtering methods are appropriate and effective.
- Appropriate filtering is in place to ensure that learners are unable to access terrorist and extremist material online through academy servers.

- All staff and pupils activity on the academy computers is monitored through Securus software. Misuse or unacceptable / inappropriate behaviour whilst using the academy computers is logged and a member of the Senior Leadership Team is notified.

Managing emerging technologies

- Emerging technologies are examined for educational benefit on a case by case basis.
- Mobile phones, tablets (other than those provided by the academy) and e-readers are not used during lessons or formal school time. Any mobile phone brought into the academy by a child for a specific purpose remains the sole responsibility of that child. The school takes no responsibility for the loss or damage of that phone. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy decisions

Authorising Internet access

- All staff read and sign the 'Acceptable ICT Use Agreement' before using any academy ICT resource.
- The academy keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves or a pupil's access is withdrawn.
- All pupils in the academy read and agree to an acceptable use policy when they join the academy.
- Access to the Internet will be supervised by a teacher or responsible adult.

Assessing risks

- The academy takes all reasonable precautions to ensure that user's access only appropriate material by using Atomwide's filtering system.
- The academy audits ICT provision on an ongoing basis to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse is referred to the head teacher.
- Complaints of a child protection nature are dealt with in accordance with the academy's child protection procedures.

- Pupils and parents are informed of the complaints procedure.

Communications

Introducing the e-safety policy to pupils

- E-safety rules are posted in all networked rooms and discussed with the pupils at the start of each term.
- Pupils are informed that network and Internet use will be monitored.
- As part of the National Curriculum and skills development, our pupils and their parents are informed of the child exploitation and online protection centre: www.thinkuknow.co.uk
- Children are educated in ways to stay safe online and how to act responsibly whilst online and using mobile devices.

Staff and the e-Safety policy

- All staff have copies of the academy's e-Safety Policy and know its importance.
- Staff are aware that Internet traffic can be monitored and traced to the individual user.
- Awareness raising training is delivered to all staff about what terrorist and extremist material looks like.
- Colleagues understand what terrorist/extremist material looks like and are confident to share concerns through the appropriate processes if they do encounter this material.

Enlisting parents' support

- Parents' attention is drawn to the academy's e-Safety Policy in newsletters, the school brochure and on the school Web site.

This policy will be reviewed, every two years, by the governors and staff as part of the whole academy policy review cycle. In addition, the subject leaders for Computing will review and update the policy annually in light of new guidance.

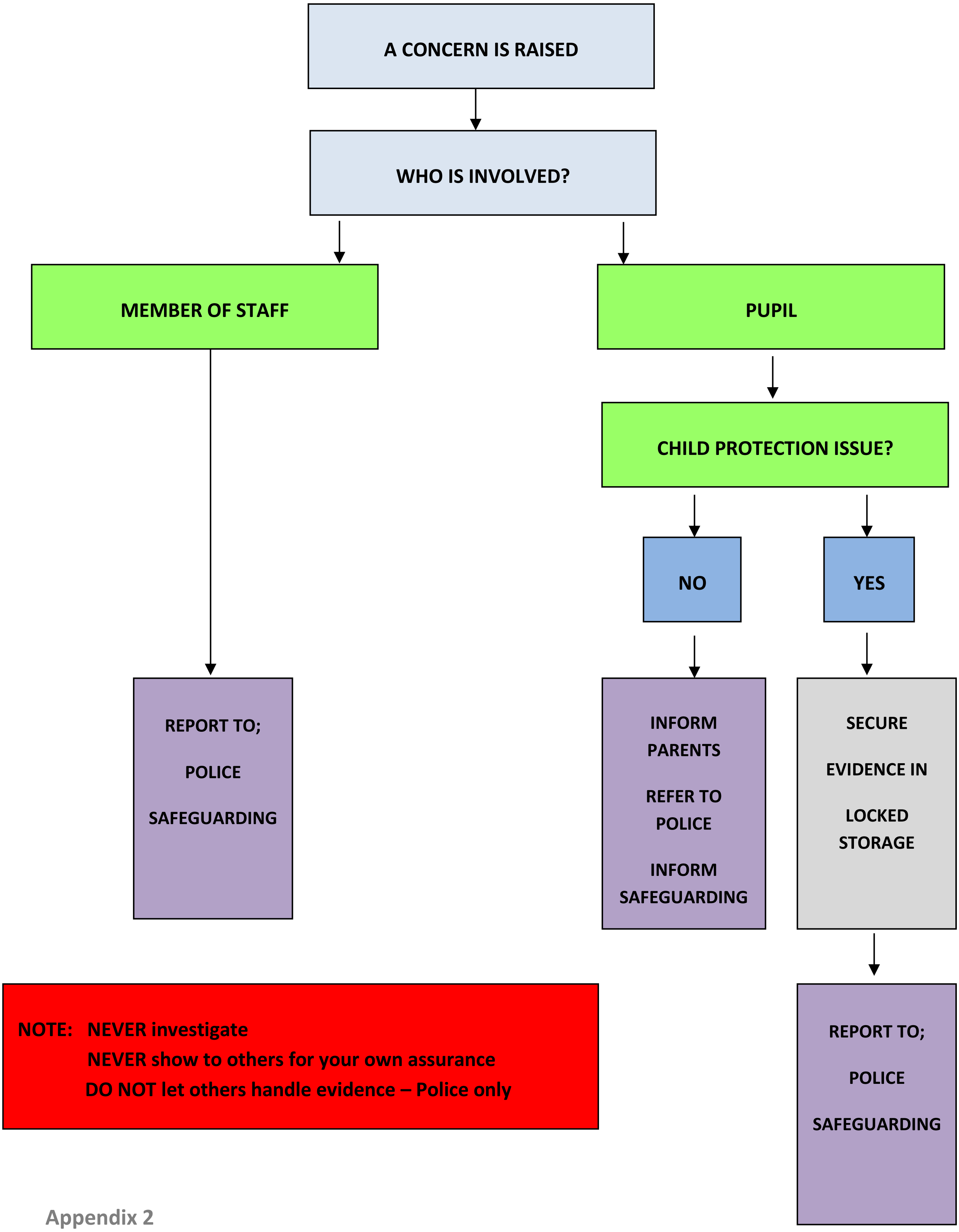
Policy reviewed March 2017

To be reviewed March 2018

(Based on Monmouthshire CC Policy document)

Appendix 1

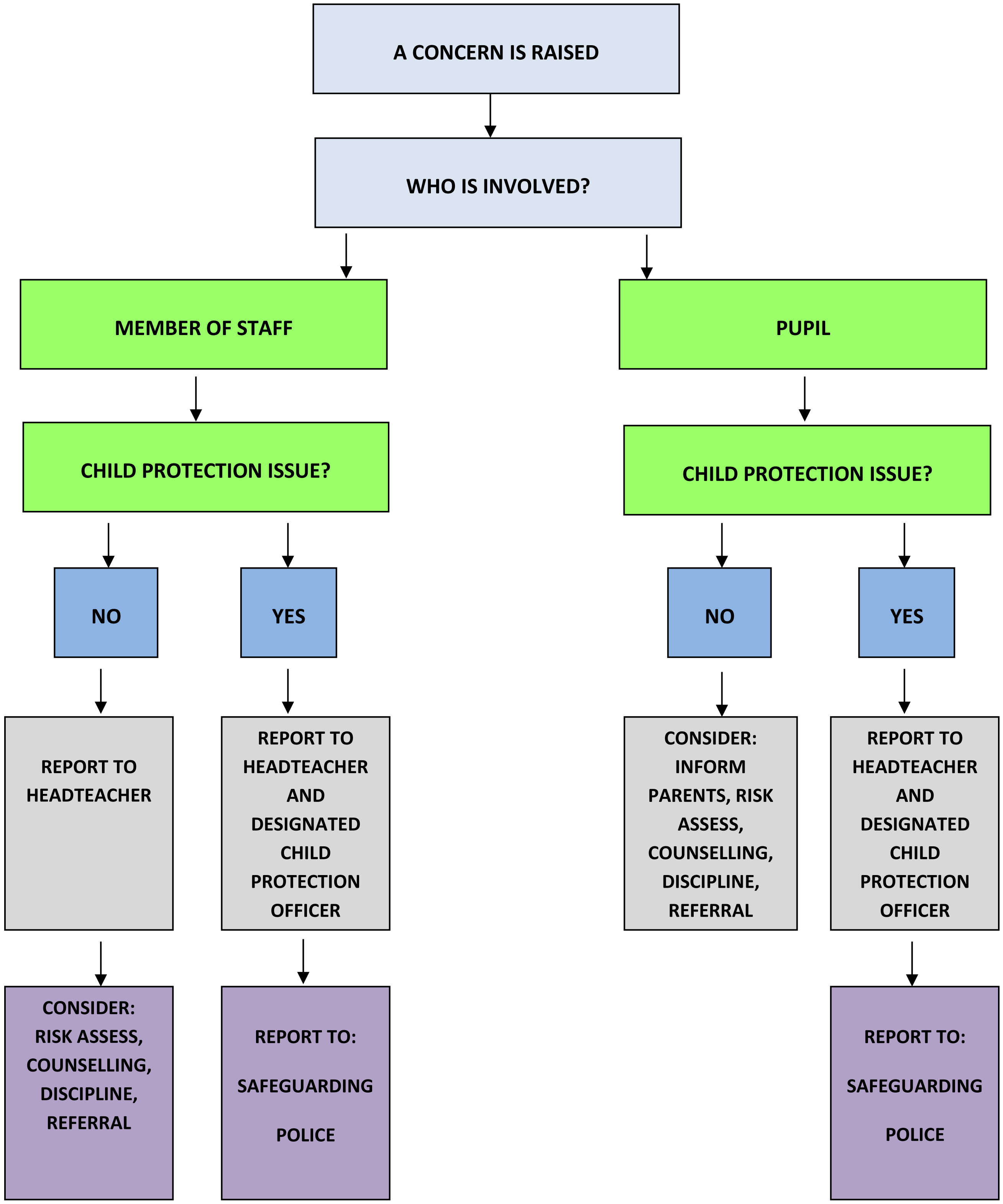
ILLEGAL ACTIVITY FLOWCHART



NOTE: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only

Appendix 2

INAPPROPRIATE ACTIVITY FLOWCHART


A CONCERN IS RAISED
WHO IS INVOLVED?
MEMBER OF STAFF
PUPIL
CHILD PROTECTION ISSUE?
CHILD PROTECTION ISSUE?
NO
YES
NO
YES
REPORT TO HEADTEACHER
REPORT TO HEADTEACHER AND DESIGNATED CHILD PROTECTION OFFICER
CONSIDER: INFORM PARENTS, RISK ASSESS, COUNSELLING, DISCIPLINE, REFERRAL
REPORT TO HEADTEACHER AND DESIGNATED CHILD PROTECTION OFFICER
CONSIDER: RISK ASSESS, COUNSELLING, DISCIPLINE, REFERRAL
REPORT TO: SAFEGUARDING POLICE
REPORT TO: SAFEGUARDING POLICE

IF YOU ARE IN ANY DOUBT CONSULT THE HEADTEACHER, DESIGNATED CHILD PROTECTION OFFICER OR SAFEGUARDING

Appendix 3

RISK LOG
(with a couple of examples)

No	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	e-safety officer/IT support
2	Internet browsing	Access to inappropriate/illegal content - pupils	2	3	6	
3	Blogging	Inappropriate comments	2	1	2	
4	Blogging	Using copyright materials	2	2	4	
5	Pupil laptop	Taking laptops home - access to inappropriate/illegal content at home	3	3	9	
6	Pupil Tablet	Taking laptops home - access to inappropriate/illegal content at home	2	3	6	

Likelihood: how likely is it that the risk could happen (foreseeable)

Impact: what would the impact be to the academy (eg this could be I terms of legality, reputation, complaints from parents, reporting in the press etc)

Likelihood and Impact are between 1 and 3, 1 being the lowest
Multiply Likelihood and Impact to achieve score

LEGEND/SCORE

1-3 = Low Risk
4-6 = Medium Risk
7-9 = High Risk

Owner: The person who will action the risk assessment and recommend mitigation to the Headteacher/Governing Body.
Final decision rests with the Headteacher and Governing Body