Alexander Hosea Primary School

'Roots to grow, wings to fly'

Online Safety Policy

Aims

The aim of this policy is to enable our pupils and staff to benefit from the advantages of online technology whilst keeping them safe from potential threats.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems. The policy aims to promote Online Safety behaviour, it includes incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

We aim to work with staff, pupils, parents, governors and technical support to ensure the safety (including Online Safety) of members of the school community. The Headteacher, the designated person for child protection, is trained in Online Safety issues. All staff receive annual training in term 1 covering online safety issues. All staff are trained on child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

Parents / Carers

Parents and carers have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents to do this by providing:

- Clear acceptable use policy guidance
- An agreement for parents to read through with their child
- An online safety meeting for parents
- Sharing information through a page on the school website

Governors and staff

There is training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the acceptable use policies.

- An audit of the Online Safety training needs of all staff is carried out annually.
- All staff have regular and relevant Online Safety training or updates.
- This policy and its updates shared and discussed in staff and governor meetings.
- The Computing leader and Computing governor communicate relevant information about Online Safety issues. Staff act as good role models in their own use of ICT.

Pupils

The education of pupils in Online Safety is an essential part of our school's Online Safety provision. All year 1 and year 3 pupils and pupils new to the school are required to sign an online safety agreement. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

- As part of the new Computing Curriculum, there is a scheme of work based around staying 'SMART' (Safe, Meeting, Accepting, Reliable, Tell)
- Key Online Safety messages will be taught continually as well as reinforced annually through an assembly and Online Safety week.
- Pupils are helped to understand the acceptable use policy and act accordingly by parents and staff
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems are posted in all rooms where ICT is used.
- Pupils report any concerns they have regarding staying safe online to a member of staff.
- Misuse of computers is treated seriously and can result in a pupil being excluded from using ICT equipment for a set period of time.

Curriculum

Online Safety is a focus in all relevant areas of the curriculum.

- In lessons where internet use is pre-planned, pupils are guided to sites checked, by staff, as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the Internet, using search engines, staff are vigilant in monitoring the content of the websites. When working in the ICT suite, staff use 'sycronise', a system which allows staff to monitor all pupils during lessons to ensure they are safe. Pupils are supervised at all times when having access to the Internet.
- Pupils use their 'SMART' training to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Development, Monitoring and Review

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of pupils, parents / carers, and all staff

Technical Roles and Responsibilities

The Local Authority provides us with technical guidance for Online Safety issues. They ensure the school's ICT infrastructure is secure and is not open to misuse or attack. As a school we comply with the e-safety technical requirements outlined in the South West Grid for Learning Security Policy and Acceptable Usage Policy. We ensure that users may only access the school's network through a properly enforced password and passwords are regularly changed.

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Through Online Safety and child protection training all staff are informed and educated about these risks.

- The risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.

- Staff ensure that pupils also act in accordance with their acceptable use policy.
- Pupil's work is only published on a public web site with the permission of the student and parents or carers. It is important that where an image is used, this is with parental consent and names must not be used. Parental consent is sought via a form, which is issued and completed before a child starts at the school. A record of all children whose images are not to be used is kept securely in the school office for reference.

Safe Use of Communications Technologies

A wide range of communications technologies have the potential to enhance learning

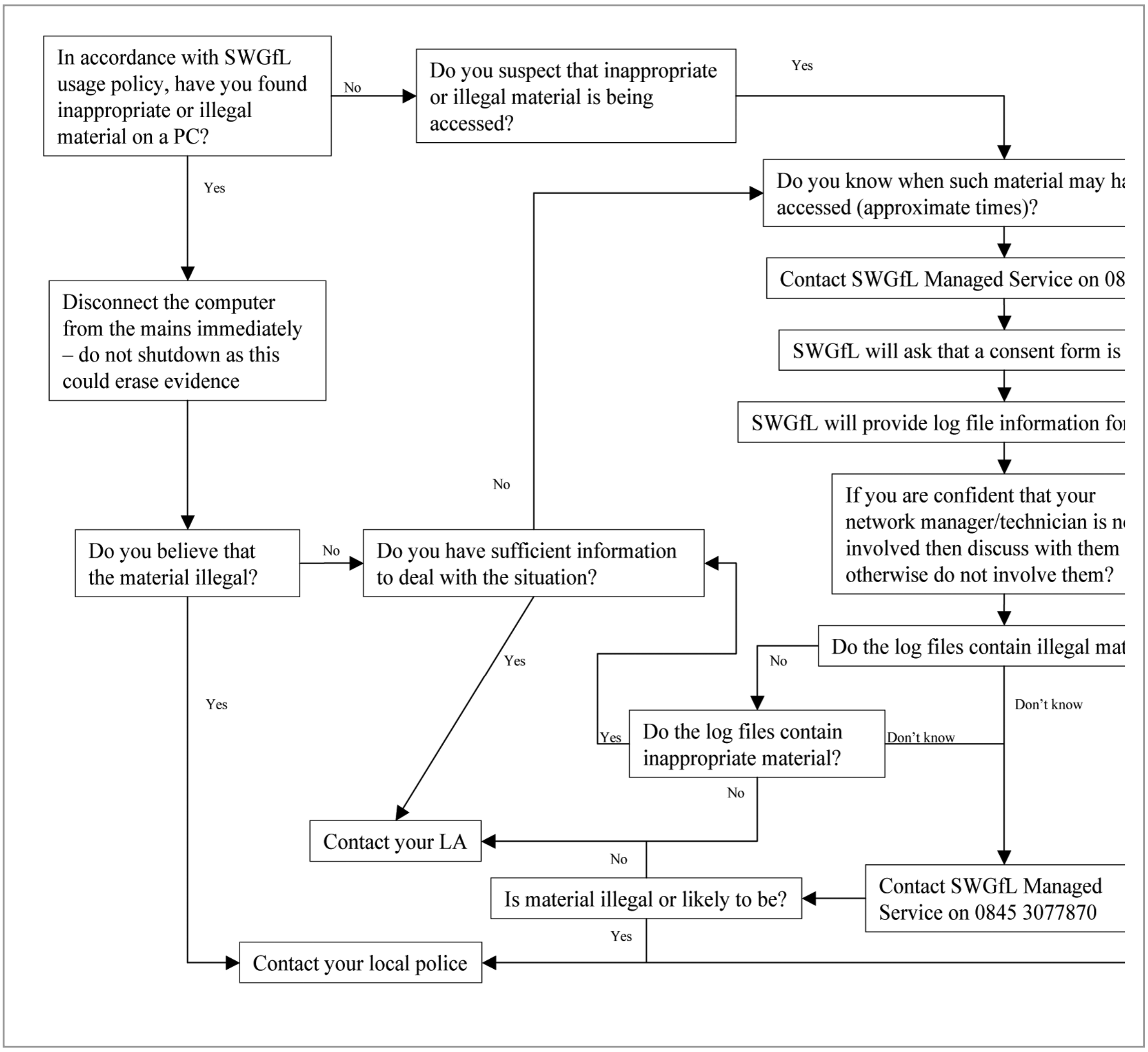
- The official school email service is used for communications between staff, and with parents/carers and pupils, as it provides an effective audit trail.
- Any digital communication between staff and pupils / pupils or parents / carers must be professional in tone and content. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils are not allowed to bring mobile phones to school. They are taught about how to use them safely as part of cyber bullying.
- Mobile phones are not to be brought into school by visitors. They must be locked securely in the lockers provided before entering the premises. Staff may keep mobile phones in a secure place and these must only be accessed during non-contact times when children are not present.

Responding to incidents of misuse

If despite our best efforts pupils misuse the Internet, digital images or other IT equipment in school, it is the supervising staff's responsibility to report the incident to Ms Quest as well as inform parents or carers. A form will be completed detailing the incident; a copy will be given to the pupil and all relevant staff to the incident. Pupils can be banned from using the relevant piece of equipment as detailed on the form. A time limited ban on using the Internet may be applied. Parents will be informed and these incidents will be logged and monitored by SLT, governors and the Computing leader.

We expect all members of the school community to be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy take place. If any apparent or actual misuse appears to involve illegal activity, this will be taken seriously and the flow chart below will be consulted.

Appendix A



In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may h
accessed (approximate times)?
Contact SWGfL Managed Service on 08
SWGfL will ask that a consent form is
SWGfL will provide log file information fo
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
No
If you are confident that your network manager/technician is n
involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal mat
Yes
No
Yes
Don't know
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

If members of staff suspect that any misuse might have taken place it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the South West Grid for Learning "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" will be followed. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Conclusion : This policy is to be read in conjunction with all other school policies. It will be reviewed in two years

Equalities Impact Assessment (EIA)

This policy has been screened to ensure that we give 'due consideration' to equality of opportunity and has been agreed and formally approved by the appropriate reviewing and ratification Committee.

Author	Alice Sabanowski	**Date reviewed**	September 2015
Position	ICT Leader	**Date ratified**	October 2015
Document status	Ratified	**Next review date**	September 2017
Version (from 2017)	1	**Reviewing committee**	H,S,W&P