# PARK SCHOOL
# E-SAFETY POLICY

Reviewed: September 2021 Next review: September 2022

## INTRODUCTION

Digital technology has become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

- The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and children learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the people in a child's education including the Head teacher, Council of Governance, class teachers, support staff, parents, members of the community and the children themselves.

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision, to build children's' resilience to those to which they may be exposed, so that they have the confidence and skills to face and deal with them.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of and sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable online gaming
- An inability to evaluate the quality, accuracy and relevance of information on the internet

- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and safeguarding policies).

This policy applies to all members of the school community (including staff, children, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of children when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour.

## Roles and responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

## Council of Governance:

Council are responsible for the approval of the E-Safety Policy and for its regular review and one member takes on the responsibility of E-Safety. This role will include:

- meeting with the Headteacher and class teachers when needed
- monitoring of e-safety incidents in our bullying log
- monitoring of filtering / change control logs
- reporting to Council annually.

## Headteacher is responsible for:

- ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the class teachers
- ensuring that the class teachers and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant and possible.
- being aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SWGfL flow chart on dealing

with e-safety incidents – included in a later section – "Responding to incidents of misuse") and the Whistle-Blowing Policy.

## Technical staff

The school uses a managed ICT service (Electrowise), which carries out all the e-safety measures that would otherwise be the responsibility of the school's in house technical staff, as suggested below. It is also important that the managed service provider is fully aware of the SWGfL Security Policy and Acceptable Usage Policy.)

Electrowise are responsible so

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the software / system is implemented and updated when needed.

## Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of the current school e-safety policy and practices
- they report any suspected misuse or problem to the Headteacher
- digital communications with children's (email / Virtual Learning Environment (VLE) / voice) should be on a professional level *and only carried out using official school systems, via children's emails and google classroom*
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- children understand and follow the school e-safety and acceptable use policy
- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra -curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned, children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

## Designated Safeguarding Lead

Should be trained in e-safety issues and be aware of the potential for safeguarding and serious 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
- cyber-bullying

(NB. It is important to emphasise that these are safeguarding and child protection issues, not technical issues, simply that the technology provides additional means for the safeguarding and child protection issues to develop.)

## Children need to:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand and support their children in the safe use of the internet and digital devices, including links in the weekly newsletter.
Parents and carers should discuss any concerns with their child's class teacher or the designated safeguarding lead.

## Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum:

- In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use. Unsuitable material that is found in internet searches will be dealt with in a sensitive manner.
- Where children are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. Foxes class teacher to check search history on Chromebooks every week.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can temporarily remove those sites from the filtered list for the period of study.
- Children should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

## Staff must ensure that they

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Ensure that personal or sensitive data regarding the school or its Children, families or other staff members is stored on USB drives
- Staff to adhere to the Acceptable Usage policy

**Communications**

A wide range of rapidly developing communications technologies has the potential to enhance learning. Staff should always be sensitive to the context when recording. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| | **Staff & other adults** | | | | **Children** | | | |
|---|---|---|---|---|---|---|---|---|
| **Communication Technologies** | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permissio n | Not allowed |
| Mobile phones may be brought to school | X | | | | | | X | |
| Use of mobile phones in lessons | | X | | | | | | X |
| Use of mobile phones in social time | X | | | | | | | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Taking photos on mobile phones | | X | | | | | | X |
| Taking photos on other camera devices | X | | | | | | X | |
| Use of personal email addresses in school, or on school network | X | | | | | | | X |
| Use of school email for personal emails | | | | X | | | | X |
| Use of chat rooms / facilities | | | | X | | | | X |
| Use of instant messaging | | X | | | | | | X |
| Use of social networking sites | | X | | | | | | X |
| Use of blogs | X | | | | | | X | |

## When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and children should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored, including children's emails
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and children or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications should only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses can be used
- Children should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

## Cameras, mobile phones and image recording in school

Photographs and videos of children taken for school and family use are a source of pleasure and pride and enhance children's self- esteem. The school policy around image taking at school is:

- School decides when recording images of children in school is permitted and parents must follow staff guidance.
- Photographs and videos may be taken at **school events** by family members for their own ***personal use***. **Such photographs and videos cannot be passed on or sold or put**

**on the internet (including social networking sites) without consent.** Failure to comply is a breach of the Data Protection Act.

- Consent must be given by parents whose children are included in the image, even if unintentionally in the background.
- Children changing clothes, wearing swimwear or wearing underwear must ***never*** be photographed or videoed.
- Images of children taken during the school day (not including school events – see above) may only be taken on personal devices with the permission of the head teacher. Any images should be transferred to the school network as soon as possible and the images saved on the personal device deleted.

## Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

The school policy restricts certain internet and I.T. equipment usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Not acceptable | Not acceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | child sexual abuse images | | | | | x |
| | promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation | | | | | x |
| | adult material that potentially breaches the Obscene Publications Act in the UK | | | | | x |
| | criminally racist material in UK | | | | | x |
| | pornography | | | | x | |
| | promotion of any kind of discrimination | | | | x | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | promotion of racial or religious hatred | | | | x | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | x | |
| | any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | x | |
| Using school systems to run a private business | | | | | X | |
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | | | | | X | |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) | | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | | X | |
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet | | | | | X | |
| On-line gaming (educational) | | | X | | | |
| On-line gaming (non-educational) | | | | | X | |
| On-line gambling | | | | | X | |
| On-line shopping / commerce | | | X | | | |
| File sharing | | | X | | | |
| Use of social networking sites | | | X | | | |
| Use of video broadcasting e.g., YouTube | | | X | | | |

## Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the

policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

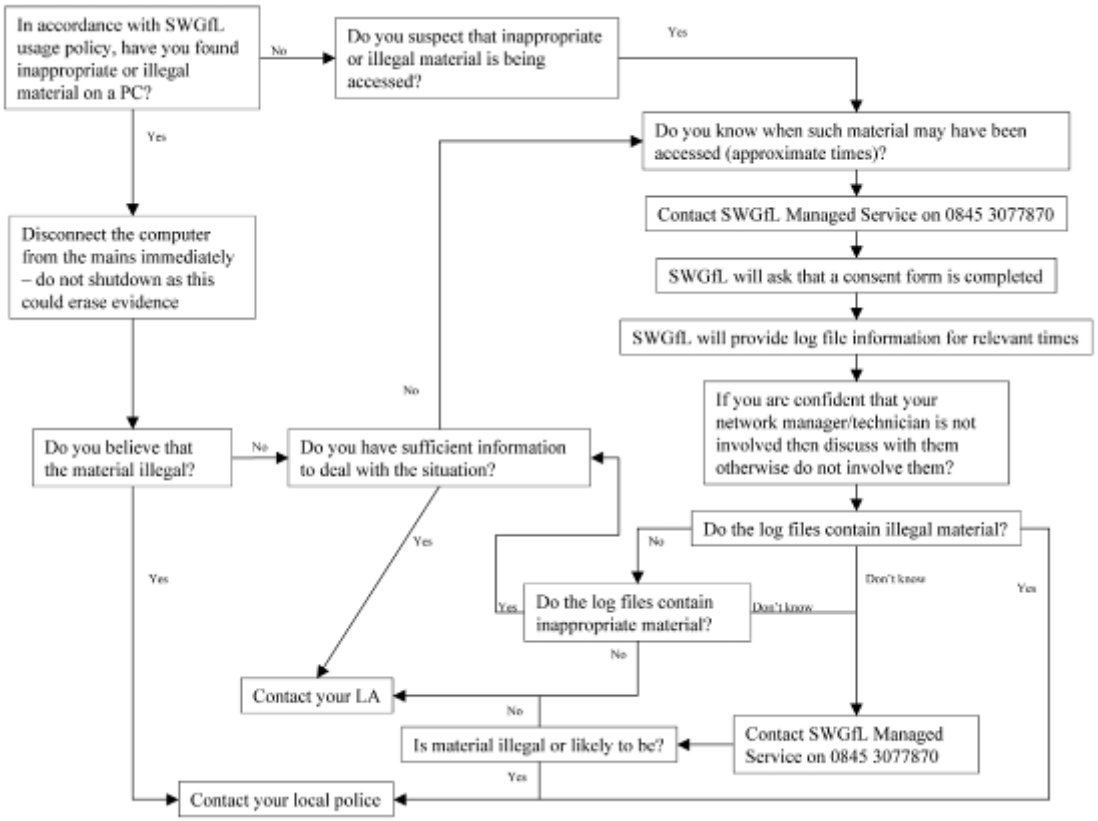
Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

See flow chart below.

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.




If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be

followed. This can be found on the SWGfL Safe website within the “Safety and Security booklet”. 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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

## Resources

http://kidsmart.org.uk/teachers/ks1/digiduck.aspx for younger children.

http://www.swgfl.org.uk/Staying-Safe/So-you-got-naked-online/So-You-Got-Naked-Online for older children and parents.

www.thinkuknow.co.uk

Amendments September 2021

1. Page 3 Amendment to statement ‘that parents using their skills to do tech work’ to ‘Electrowise’
2. Page 6 Amendment to permissions, Taking photos on mobile phones, allowed in certain circumstances
3. Page 7 Amendment to statement that staff should not use personal devices to take photographs’ amended to read: ‘Images of children taken during the school day (not including school events – see above) may only be taken on personal devices with the permission of the head teacher. Any images should be transferred to the school network as soon as possible and the images saved on the personal device deleted.’
4. Page 7 Amendment to permissions, Use of school email for personal emails – staff not allowed to use schools email for personal emails.
5. Page 7 Amendment to permissions: Use of social networking sites – allowed in certain situations.