# Park School for Girls

# e-Safety Policy

## This policy applies to the whole school including EYFS

September 2018

**1. Introduction and Aims**

Information and Communications Technology (ICT) covers a wide range of resources including: web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms (MLE) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

At Park School for Girls we understand the responsibility to educate our students in e-Safety issues; teaching them the appropriate behaviours and critical thinking, to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet. New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils 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. This e-safety policy will help to ensure safe and appropriate use. 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 or 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 video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- 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 read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour, Child Protection and Mobile Phone Use. (Also, see ICT and safeguarding policies as well as the staff handbook pages 6-7)

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

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use. We have had and will continue to have the community police visit and deliver workshops to our pupils regarding being safe on line especially on social media and cyber-bullying particularly when they are not in school. We plan to take advantage of their services to run workshops on internet safety for parents during this academic year.

**2. Roles and Responsibilities**

E-Safety is recognised as an essential aspect of strategic leadership at Park School for Girls. All staff on the Child Protection team will receive CEOP (Child Exploitation and Online Protection) training.

Androulla Nicholas (Headteacher) has overall responsibility for safeguarding as the DSL. Anne Lacey is the Deputy DSL. Christina Clayden is the Deputy Safeguarding Lead for the Preparatory School, [in her absence it is Mrs Muir] and Erin Muir is also a named staff member to whom children can report any safeguarding concerns. Erin Muir is the named staff member for e-safety.

It is the role of these staff members to keep abreast of current issues and guidance through organisations such as Redbridge Local Authority, NSPCC, Becta, CEOP (Child Exploitation and Online Protection), and Child Net. The Head teacher ensures Senior Management and

Governors are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours of the pupils in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community (see appendices)
- their role in providing e-safety education for pupils.

Staff are to be reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction

Managing the school e-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be shared with staff, including the acceptable use policy as part of their induction. The policy will also be available for pupils and parents to read on our school website.
- E-safety posters will be prominently displayed.

**3. Curriculum**

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new ways to promote e-safety.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.
- Mrs Atutonu includes staying safe online in her lessons with the senior school. This includes safety using social media and cyberbullying. They are taught about the importance of keeping their personal information private and not disclosing it with anyone online.
- Internet safety is taught in ICT lessons every year by the Preparatory School staff.
- The school will participate in Internet Safety day in February
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.
- We will regularly distribute questionnaires to children to monitor their understanding of e-safety.

- Pupils are aware through PSHEC lessons, of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- We provide opportunities within a range of curriculum areas to teach about e-safety.
- Rules for the use of ICT systems and the Internet are posted in school.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.
- Students are taught of the dangers of sharing personal information on social media.

**4. Managing Internet Access**

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people.

- Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.
- Our internet access is currently controlled by Impero and Computer Talk maintains our network. In August 2017, the school purchased 'Surf Protect' by ESA. This software blocks any unauthorised websites being accessed by staff and students. Our ICT coordinator is able to control what staff and pupils access and block and unlocks sites accordingly. Whenever a problem arises the e-safety coordinator and ICT coordinator meet briefly to discuss solutions.
- It is the responsibility of the school, by delegation to Computer Talk, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Any changes to filtering must be authorised by a member of the senior leadership team.

**5. Acceptable Usage Policy**

Introducing the e-Safety policy to pupils

- E-Safety rules are displayed in the ICT suite and discussed with the pupils at the start of each term. All staff are aware that at least one dedicated e-safety lesson must be taught each term and at relevant points throughout e.g. during PSHEC lessons//anti-bullying week/Safer Internet Day.
- Pupils will be informed that network and Internet use will be monitored**.**
- The school is vigilant when conducting 'raw' image search with pupils e.g. Google image search
- Pupils are required to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme

Staff and the e-Safety policy

- All staff must sign the Staff AUP and a copy is kept on file.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- All members of staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Any laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Parents and the e-safety policy

- All parents will be asked to sign the Acceptable Use Agreement (AUA) for pupils giving consent for their child to use the Internet in school by following the school's e-Safety guidelines and within the constraints detailed in the school's e-Safety policy.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- Parents are encouraged to look at the school's e-safety policy and the pupil 'Acceptable User Agreements' (for Preparatory School and the Upper School)

**6. Security and Data Protection**

The school and all staff members comply with the Data Protection Act 1998. Personal data will be recorded, processed, transferred and made available according to the act. This is due to be replaced with a new government act in 2018. Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have secure passwords which are not shared with anyone. All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy.

**7. e-Safety Complaints/Incidents**

As a school we take all precautions to ensure e-safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device outside of school. As mentioned in section 3 – Curriculum, students are taught in formal e-safety lessons in ICT about what they can do to protect themselves on their personal devices. We do used local resources such as the police to do workshops with the students. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Headteacher. Incidents should be logged and the flowchart (See Appendix) for managing an e-safety incident is to be followed. It is important that the school works in partnership with pupils and parents to educate them about Cyber bullying and children, staff and families need to know what to do if they or anyone they know are a victim of Cyberbullying. The e-safety coordinator plans to run an e-safety workshop for parents within this academic year.

**8. Communication**

Transparency, openness and appropriate professional purpose must underpin all academic and pastoral interaction with pupils via electronic and digital means.

<u>Email</u>

- Digital communications with pupils should only be via email, or a school mobile phone and be on a professional level and only carried out using official school systems (see staff guidance in child protection policy).
- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems) or Outlook;
- Staff should only use school email addresses to communicate with pupils and parents.
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.
- School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ pupils.

- All staff using email need to be aware of the less formal style that can characterise this form of communication and should ensure that emails do not convey an inappropriate tone. Repeated email communication is a particular cause for concern, as it can spiral out of control almost unnoticed by those conducting it.

Mobile Phones

- **School mobile phones** only should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices.

- Pupils' mobile telephone numbers and text messages should not be used and mobile phone numbers of pupils must not be stored on a personal mobile and pupils should not ever have access to teachers' personal mobile numbers (Form Tutors and other pastoral staff may keep confidential paper copies of pupil's telephone numbers with the prior approval of the DSL, for exceptional pastoral circumstances). (Safeguarding Policy)

- **Staff** should not be using personal mobile phones in school during working hours when in contact with children. (See Code of Conduct)
- **Students** should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school. Students should hand their mobile phones to their form teacher during morning registration and they will be given back during form time at the end of the day.

Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.
- **Staff** must consider carefully the public nature of such sites and decide if it is appropriate to join.
- **Staff** must not mention the name of the school on your personal sites and ensure that any pictures of the school or its pupils are removed.
- **Staff** users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog**.**
- **Students/Parents/carers** should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.
- **Students** will be taught about e-safety on social networking sites as we accept some may use it outside of school. The students all receive formal lessons during ICT. (See Section 3 – Curriculum)

- We encourage staff to ensure that they have the correct security and privacy settings on sites. That they are aware of the information about themselves that may be available on the web and social network sites and that may be open to parents, pupils and colleagues. If they have any concerns that anything exists that could compromise their professional reputation, or undermine the reputation of the School – they must inform the DSL without delay. Training and privacy settings on social networking sites and their safe use can be obtained from the Bursar and please refer to the school's IT policy on social media. Privacy settings must be updated regularly as social media can change its operating procedures. It is the responsibility of each member of staff to check their settings are up to date. (See code of Conduct)
- Contact between staff and current pupils on Facebook and other social network sites is prohibited. Never allow an existing pupil to join your circle of "Friends".

Digital Images

The school are keen to record students working and in other school activities in picture and video format.

Such filming will only be taken on school i-pads. The i-pads are physically stored securely by the Bursar and will be issued to staff on request. Each i-pad is secured by a passcode known to staff but not students.

If a teacher is using i-pads in a lesson or activity they will remain fully diligent to ensure that students stay on task and no unauthorised films or photos are taken. Devices will be returned to the Bursar at the end of the lesson and the images will be promptly transferred to the school network and deleted from the device. Unauthorised photos will be deleted and the staff made aware.

- The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list can be obtained from the data office.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the parent, and the Head Teacher.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and parent mail which are used to inform, publicise school events and celebrate and share the achievement of students.

All pupils and staff are encouraged to report any concerns about the misuse of technology to the Headteacher. The use of cameras, cameras on mobile phones and/or iPads by pupils is not allowed without express permission from a member of staff. Staff may only use cameras, cameras on mobile phones and/or iPads in a manner that is strictly in accordance with the guidance in this policy and which, in any case, does offend or cause upset. The misuse of

cameras by staff or pupils in a way that breaches our Staff Code of Conduct, Safeguarding and Anti-Bullying policy is always taken seriously and may be the subject of disciplinary procedures.

If we discover that a child or young person is at risk as a consequence of online activity, this will be managed in line with our safeguarding procedures and we may seek additional assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any adult, child or young person who misuses technology in this way.

Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. It will be handled according to the anti-bullying policy and may be treated as a safeguarding concern.

All pupils must allow staff access to images stored on mobile devices and/or cameras and must delete images if requested to do so.

The posting of images and video which in the reasonable opinion of the Headteacher are considered to be offensive on any form of social media or websites such as YouTube etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using school or personal facilities.

There is a separate policy on taking, storing and using images of children in the EYFS

EYFS/KS1
At Park School, for Reception and Key stage 1 Classes we use photographic images to record children's progress and development during their time in the EYFS and KS1. When parents sign the terms and conditions document on joining the school they agree to the use of their children's images being used for publicity and promotion of the school. They can opt out of that permission if they choose to. Children are only photographed with the consent of parents/carers. Written permission is obtained when a child joins the school

At Park School, Reception and Key Stage 1 Class photographs are normally taken and used for the following purposes:

- Displays of the children's work/activities
- Personal records of achievement for each child
- School web site and Newsletter

<u>Appendices</u>

1. Acceptable use of ICT agreement – Preparatory Department.

2. Acceptable use of ICT agreement – Upper School.

3. Letter to parents about Acceptable use agreement.

4. Acceptable use of ICT agreement – Staff/Governors.

5. Flowchart for managing e-safety incident (not involving illegal activity).

6. Flowchart for managing an e-safety incident involving illegal activity.

# PARK SCHOOL FOR GIRLS

## Acceptable Use of ICT Agreement/E-Safety
## Preparatory Department

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will not bring software, CDs or ICT equipment into school without permission.
- I will only use the Internet after being given permission from a teacher.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not use technology in school time to arrange to meet someone unless this is part of a school project approved by a teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my e-Safety.

**Signed …….**

**Date …….**

# PARK SCHOOL FOR GIRLS

## Acceptable Use of ICT Agreement/E-Safety
## Upper School

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.

- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.

- I will immediately report any damage or faults involving IT equipment, however this may have happened.

**Signed ……..**

**Date …….**

**PARK SCHOOL FOR GIRLS**
**20-22 Park Avenue**
**Ilford**
**IG1 4RS**
**admin@parkschool.org.uk**
**Headteacher: Mrs. A. Nicholas**
**June 2017**

Dear Parents/Carers,
ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in schools. We expect all children to be safe and responsible when using any ICT. Please read and discuss with your child the E-Safety rules overleaf and return this sheet signed by both you and your child. If you have any concerns or would like some explanation please contact your child's class teacher.
This Acceptable Use of ICT Agreement is a summary of our e-Safety Policy, which is available in full on our website or as a hard copy in our Office/Reception.

Yours sincerely,

**A. Nicholas**
**Headteacher**

**Pupil:**
I have read, understood and agreed with the Rules for Acceptable use (AUA) of ICT.

**Signed ……. (child)**

Parent's/Carer's Consent for Internet Access
I have read and understood the school rules for Acceptable Use of ICT (AUA) and give permission for my son / daughter to access the Internet in school. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.
I agree that should my son/daughter need to access e-folio at home or anywhere else, that I will take all reasonable precautions to ensure he/she cannot access inappropriate materials and that he/she will use the computer in an appropriate manner.

**Signed…….…… (parent/carer) Date…….**

# PARK SCHOOL FOR GIRLS

## Acceptable Use of ICT Agreement
## Staff, Governor and Visitor
## Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Androulla Nicholas, Headteacher or a member of the CP team.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that personal data (such as data held on Scholar Pack) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

- I will not use or install any hardware (including USB sticks) or software without permission from the e-safety co-ordinators.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

- I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …… Date ……

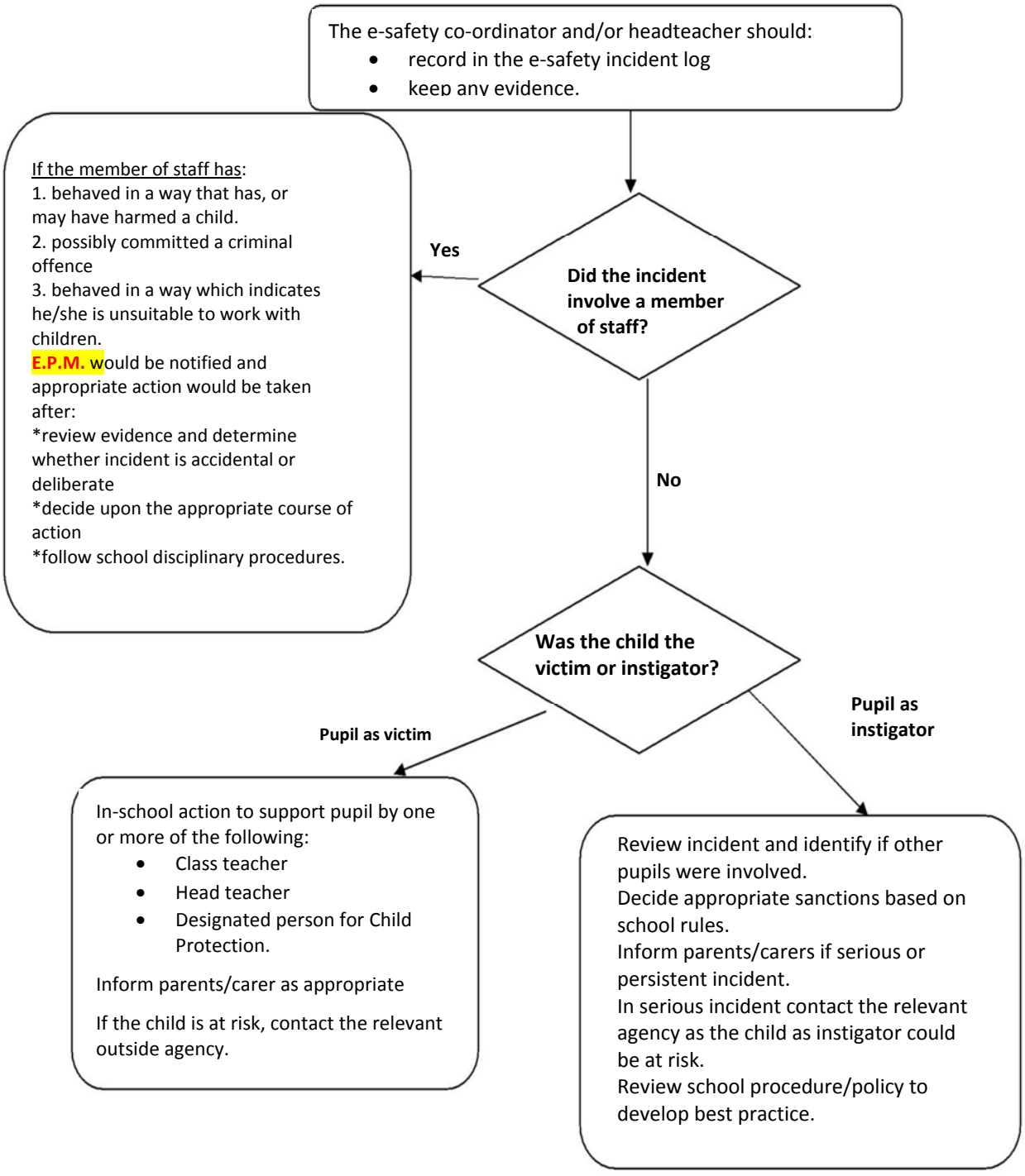
Full Name ……..... (printed)

Job title: ……..

# Flowchart for managing an e-safety incident not involving any illegal activity

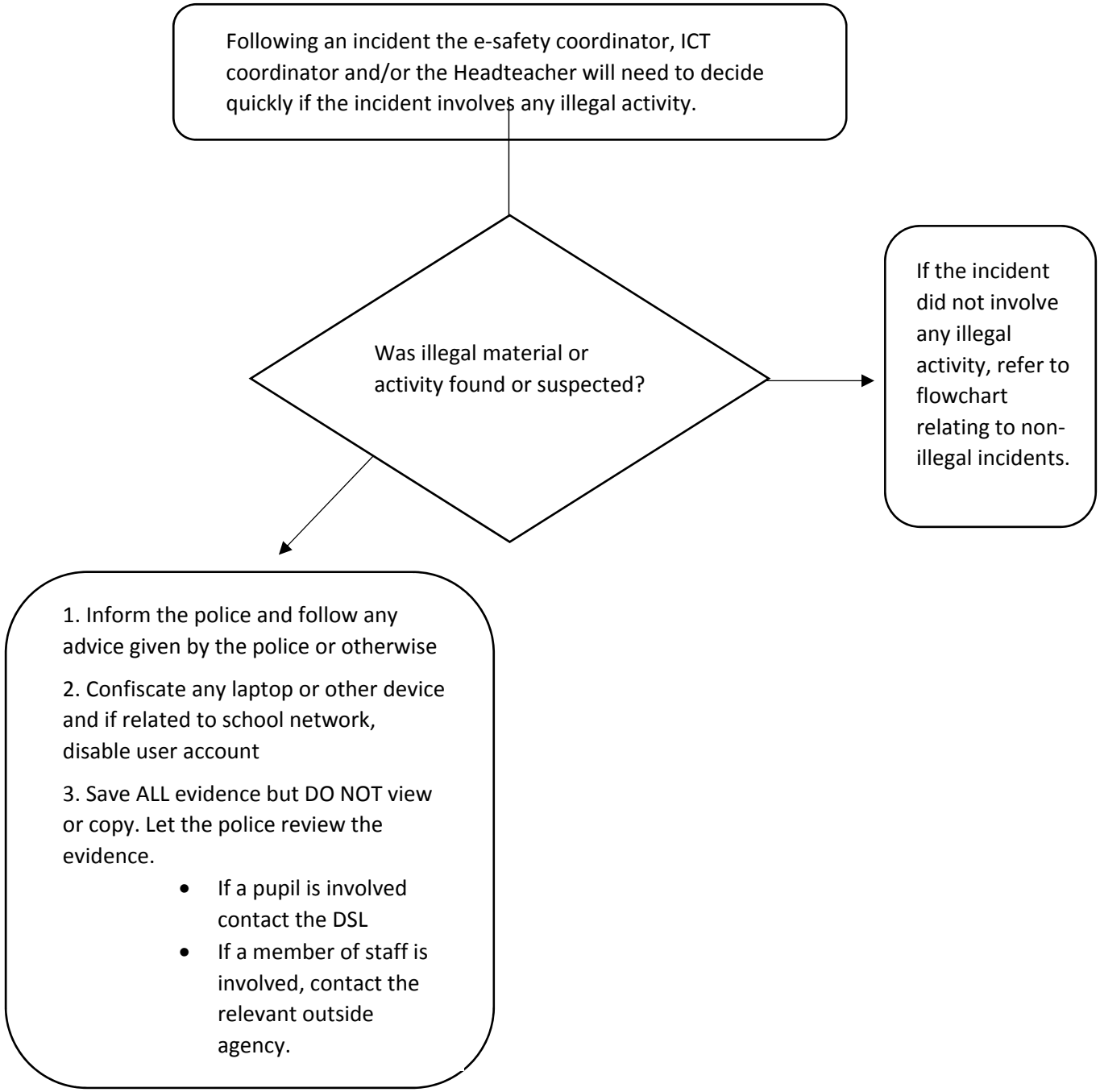
Incidents not involving any illegal activity, such as:

- using another person's user name and password
- accessing websites which are against school policy
- using a mobile phone to take video during a lesson
- using the technology to upset or bully (in extreme cases this could be illegal)



# Flowchart for managing an e-safety incident involving illegal activity

**Illegal means something against the law, such as:**
**□ downloading child pornography □**
**□ passing onto others images or video containing child pornography**
**□ inciting racial or religious hatred**
**□ promoting illegal acts**



# Park School for Girls
# e-safety incident log

**Details of ALL e-safety incidents to be recorded in the incident log by the e-safety coordinator or the ICT coordinator. This incident log will be monitored half-termly by the e-safety coordinator, ICT coordinator and/or the Headteacher.**

| Date and time | Name of pupil or staff member | Room and computer/device number | Details of the incident (including evidence) | Actions and reasons |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Revised by the Mrs Muir and Mr Fleming** **September 2018**

**Approved by Chair of Governors** **Mr Smith** **September 2018**

**Date for review** **September 2019**

September 2018