Khaya Home Limited

POLICY NO 7

KHAYA HOME

Policy & Procedure
E-Safety

Completed March 2024 – to be reviewed March 2025 – Dr Aida Lockton

CONTENTS

E-Safety Policy

1. Introduction

Internet technology, (IT), is now an integral part of young's lives and provides them with access to a wide range of information and increased opportunities for instant communication and social networking.
Using the internet can benefit young people's education and social development, but it can also present several risks. Young people are often unaware that they are as much at risk on-line as they are in the real world, and parents/carers may not be aware of the actions they can take to protect them.
It is the policy of Khaya Home Limited that the educational and social benefits of the internet should be promoted, but that this should be balanced against the need to safeguard children and young people. Khaya Home Limited policies and procedures are designed to educate children, young people and parents/carers of the risks related to internet use and what steps to take to reduce risk and deal with issues that might arise.
Staff members who work with children and young people have a role in implementing these procedures by helping the children they work with to keep themselves safe on-line and dealing with safeguarding issues arising from e-safety incidents.
This policy provides guidance to staff on how to recognise the risks of internet use and take action to reduce these risks. The guidance also sets out what actions should be taken where a child's use of the internet puts them at risk of significant harm

2. Benefits and Risks

Internet technology allows children and young people to access information, electronic communications and social networking and can support their education and social development.
However, the use of the internet can also carry inherent risks:

Content – The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children and young people. There is a danger that children and young people may be exposed to inappropriate images such as pornography, or information advocating violence, racism or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

Contact – Chat rooms and other social networking sites can pose and real risk to children as users can take on an alias rather than their real names and can hide their identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust, (known as grooming), with a view to sexually abusing them. Children and young people may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent. The internet may also be used as a way of bullying a child or young person, known as cyberbullying.

Commerce – Children and young people are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offered for good or services without seeing the fraudulent intent. Disclosing this information can lead to fraud or identity theft.

Culture – Children or young people need to be taught to use the internet in a responsible way, as they may put themselves at risk by:
Becoming involved in inappropriate, anti-social or illegal activities because of viewing unsuitable materials or contact with inappropriate people.
Using information from the internet in a way that breaches copyright laws
Uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience.

Use of mobile devices to take and distribute inappropriate images of the young person, (sexting), that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended
Children or young people may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment.
They may visit sites that advocate extreme and dangerous behaviour such as self-harm, suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children or young people may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

3. Khaya Home Limited E-Safety Strategy

Definition and Purpose
E-Safety contributes to the 'staying safe' element of good outcomes for children and young people and Khaya Home Limited promotes a service where children are able to access the internet.
The purpose of the strategy is to:
Protect children from harm.
Safeguard staff in their contact with children and their own use of the internet
Ensure that the service fulfils the duty of care to children and young people.
Provide clear expectations for staff, children and young people on acceptable use of the internet.

Elements of E-Safety
Under the strategy, Khaya provides internet access for children, young people and will ensure an 'e-safe' environment for children by:
Ensuring safe systems with safe filtering to block access to unsuitable sites.
Monitoring children's access and use of IT
Providing safe practices with e-safety policies and acceptable use agreements that set out the user's rights and responsibilities ad sanction for breach of these agreements.
Promoting safety awareness and providing guidance and information so that children and young people are taught how to keep themselves and others safe and use the internet responsibly.
Working with parents/carers to ensure e-safety messages are extended to the home environment.

E-Safety Contact Officer
Khaya Home Limited has an E-safety contact officer who takes the lead for co-ordinating the development, implementation, and review of e-safety policies within the home.
All e-safety incidents should be reported to the e-safety officer who will decide what action needs to be taken to improve e-safety practice and deal with individual incidents.
Where any e-safety incident has serious implications for the children's safety or well-being, the e-safety officer must discuss the matter with the home's Designated Safeguarding Officer, DSO, who will decide whether or not a referral should be made to Leicestershire Local Safeguarding Board and/or the police.

4. Preventative Work

Staff may have concerns about the internet use of a child or young person with whom they work, and parents/carers may express concerns themselves. It is important that staff members are aware of the key risks and safety messages for children, young people and parents/carers in order to use the internet safely so that they can advise children and parents/carers accordingly.

Key E-Safety Messages
Children and young people need to be guided on:
The benefits and risks of using the internet.
How their behaviour can put themselves and others at risk

What strategies they can use to keep themselves safe
What to do if they are concerns about something they have seen or received via the internet
Who to contact to report concerns.
That they won't be blamed if they report any e-safety incidents
That cyberbullying cannot be tolerated.
The basic principles of 'netiquette' (how to behave on the internet).
Staff should be aware that some children or young people may be more vulnerable to risk for internet use, generally those children with a high level of computer skills but coupled with poor social skills.

Safe Use of ICT
When using the internet and internet search engines, children should receive the appropriate level of supervision for their age and understanding. Search engines should have an appropriate level of filtering to block access to unsuitable sites

When using e-mail children should be taught:
- To keep messages polite
- Not to disclose personal contact details for themselves or others
- To tell their parent/carer immediately if they receive an offensive or distressing e-mail
- Not to use e-mail to bully or harass others
- Be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender

When using social networking sites such as Facebook or newsgroups and forum sites, children should be taught:
- Not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
- Not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted
- How to set up security and privacy settings on sites or use a 'buddy list' to block unwanted communications or deny access to those unknown to them
- To behave responsibly whilst on-line and keep communications polite
- Not to respond to any hurtful; or distressing messages but to let their parents/carers know so that appropriate action can be taken

When using chat rooms, children should also be taught:
- Not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
- To only use moderated chat rooms that require registration and are specifically for their age group
- Not to arrange to meet anyone whom they have only met on-line
- To behave responsibly whilst on-line and keep communications polite
- Not to respond to any hurtful or distressing messages but to let their parents/carers know so that appropriate action can be taken
- That any bullying or harassment via chat rooms or instant messaging may have serious consequences

When using web cameras, children should be taught:
- To use them only with people who are well-known to them
- Not to do anything that makes them feel uncomfortable or embarrassed
- To tell their parents/carers if anyone is trying to force them to do something they don't want to

Children or young people with Special Needs
Children or young people with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on e-safety practice as well as closer supervision. Staff may wish to discuss this with parents/carers and help them to access information and resources from specialist agencies.

5. Dealing with Specific Risks

Cyberbullying

Cyberbullying is defined as the use of IT to deliberately hurt or upset someone. Unlike traditional physical forms of bullying, the internet allows bullying to continue past school hours ad invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyberbullying is extremely prevalent as children who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bully may remain anonymous. In extreme cases, cyberbullying could be a criminal offence.

Bullying may take the form of:

Rude, abusive or threatening messages via email or text

Posting insulting, derogatory or defamatory statements on blogs or social networking sites

Setting up websites that specifically target the victim

Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail, for example 'happy slapping'

Most incidents of cyberbullying will not necessarily reach significant harm thresholds and will probably be best dealt with Khaya's own anti-bullying or acceptable use policy with the co-operation of parents/carers

Children and young people should be taught:

Not to disclose their password to anyone

To only give out mobile phone numbers and e-mail addresses to people they know

To only allow close friends whom they trust to have access to their social networking page

Not to respond to offensive messages

To tell parents/carers about any incidents immediately

Parents/carers/significant person should be taught to be vigilant about possible cyberbullying and how to work with internet and mobile service providers to cut down on the risk of cyberbullying.

Mobile phone companies can trace calls and ensure that any further calls and texts from that number are blocked

Internet service providers can trace messages being sent form a personal e-mail account and can block further e-mails from the sender.

Where bullying takes place in chat rooms, the child should leave the chat room immediately and seek advice from parents/carers, bullying should be reported to ay chat room moderator to take action.

Website providers can remove comments from social networking sites and blogs and in extreme cases, can block the bully's access to the site.

The child could exchange mobile phone numbers or e-mail addresses.

Where cases of cyberbullying involve significant harm to the victim, advice should be taken from Leicestershire Safeguarding Board.

These will be incidents where the bullying is, for example:

Extreme, threats against someone's life

Involves sexual bullying or harassment.

Continues over a period of time

Involves several perpetrators or may be gang related.

Has a considerable impact on the victim

Inappropriate Contact and Non-contact Sexual Abuse

Concerns may be raised about a child being at risk of sexual abuse because of their contact with an adult they have met over the internet. Children, young person, and parents/carers should be advised how to terminate the contact and change contact details where necessary to ensure no further contact. Parents/carers should be advised to be vigilant of their child's internet use and report any concerns of incidents.

Children and young people may also be sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the child concerned to carry out sexual acts while the perpetrator watches/records. The perpetrators may be adults but may also be peers.
In the event of an incident, the child should be taught how to use the CEOP 'Report abuse' button, (normally displayed on the screen), and parents/carers should contact the police and report the incident.
Staff and parents/carers should contact Leicestershire Safeguarding Board for advice on making a referral where there are concerns that the child:
Is being groomed for sexual abuse.
Is planning or has arranged to meet with someone they have net on-line.
Has already been involved in making or viewing abusive images.
Has been the victim of non-contact sexual abuse.

If parents/carers are aware that a child is about to meet an adult they have contacted on the internet, they should contact the police on 999 immediately.

On-line Child Sexual Exploitation (CSE)
CSE describes situations where a young person takes part in sexual activity either under duress or in return for goods, food, or accommodation. A key element of CSE is that there is a power imbalance in the relationship, for example, often the perpetrator is much older that the child, who may not be aware that they are being abused.
Staff should be aware that children can be sexually exploited on-line for example, posting explicit images of themselves in exchange for money or goods.
If staff are concerned that a child, they work with is being sexually exploited on-line, they should complete the CSE risk assessment available on the CSCB website. Where indicated by the risk assessment, staff should consider making a referral to Leicestershire Safeguarding Board and may discuss this with the E-Safety Officer and Social Worker.

Contact with Violent Extremists
Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence, use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.
Staff members need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it should be against the policy of Khaya to access such sites.
Services should ensure that adequate filtering is in place, with a review of filtering taking place whenever there is any incident of a young person accessing website advocating violent extremism.
The E-safety contact Officer should record and review all incidents to establish whether there are any patterns of extremist groups targeting children and an e-safety report should be sent to the Leicestershire Safeguarding Board.
If there is evidence that a young person is becoming deeply enmeshed in the extremist narrative, the home should seek Leicestershire Safeguarding Board and Report to 'Prevent' and try to access educational programs that prevent radicalisation.
A referral should be made to Leicestershire Safeguarding Board where the child is deeply enmeshed in the extremist narrative and there is evident that they parents/carers are involved in advocating extremist violence.

Websites Advocating Extreme or Dangerous Behaviours
Some internet sites advocate dangerous activities such as self-harming, suicide, or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.
Exposure to potentially harmful materials on-line may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people, may feel drawn to the sites which may trigger harmful or even fatal behaviours.
Staff members should provide young people with an opportunity to discuss issues such as self-harming and suicide in an open manner and support any young person who is affected by these issues.

Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.
Where staff are aware that a young person is accessing such websites and that this is putting them at risk of harm, they should consider making a referral to Leicestershire Safeguarding Board.

6. Responding to Child Protection Incidents

Role of Social Services

As the statutory agency for child protection, Social Services has the key responsibility for investigating e-safety incident where the child is thought to be at risk of suffering significant harm. Incidents where an e-safety incident raises child protection concerns will be investigated via child protection procedures. Social Services will investigate e-safety incidents that involve inappropriate internet use by members of the children's workforce where this raises concerns about the persons' continued fitness to work with children. These cases must be referred to the Local Authority Designated Officer, (LADO).

Referrals to Social Services

Whenever a professional is concerned that a young person, they work with is at risk of harm due to their internet use, they should discuss their concerns with the e-safety contact officer for their service and seek advice from the LADO.

All referrals should be made to Leicestershire Safeguarding Board using their referral form.
An e-safety incident record should also be completed and sent to Ofsted. Where there are concerns about child sexual exploitation, a CSE risk assessment should be completed and sent with the referral.

Referrals should be made where there is evidence of any of the following:
The child is in contact with unsuitable adults and is either being groomed for or is already involved in online sexual abuse, for example, via webcam.
The child is either being groomed for or involved in online child sexual exploitation.
The child is either the victim or perpetrator of extreme cyberbullying, including bullying or harassment that is sexual or racist in nature, in these cases a referral should be made for both children as Social Services will need to consider the needs of both children.
The child is in contact with violent extremists and has become enmeshed in the extremist narrative and their parents/carers may support these views.
The child persistently accesses and distributes violent, pornographic or otherwise inappropriate materials.
The child is accessing websites advocating suicide, self-harm or other dangerous behaviours and there are concerns about their emotional wellbeing.
An adult member of the child's household is accessing or distributing child sexual abuse images.

Action by Social Services

All e-safety incidents involving risk of significant harm should be dealt with via the child protection system and a strategy discussion initiated in line with the Leicestershire Safeguarding Board.
Issues that will determine whether there is a risk of significant harm will include:
The extent of harm and the level of perceived risk to the child and other children
Involvement of adults can adequately protect their child from harm and take the risks posed seriously.

Social Workers should be aware that issues around e-safety may arise during assessment of other presenting issues, for example a child who exhibits sexually harmful behaviour may be accessing adult websites, or a vulnerable child may be placing themselves at more risk through their contacts on social networking sites.

Strategy discussions should consider the following:
All available electronic evidence of grooming abuse, harassment or bullying or the distribution of inappropriate images of the child.

The involvement of any adults who pose a risk to children, whether they can be identified and what action can be taken against them.
Whether other children are involved in any abuse, either as victim or perpetrator
The needs of all children involved, including perpetrators.
Whether the matter should be investigated under the organised and complex abuse procedures where there is more than one victim or perpetrator
The nature of the risk to the child and evidence of harm
The ability of parents/carers to take action to protect their child.

The police should be involved in any strategy discussion and subsequent investigation, and where the names of any involved adults are known, the strategy team should carry out checks and gather any relevant information and may contact the Child Exploitation and Online Protection Centre (CEOP) to help trace perpetrators online.

Children known to Social Services
If during working with a child a social worker becomes aware of a serious e-safety incident that has happened at home and which raises child protection concerns, the social worker should complete an e-safety incident report.
Social Workers need to work closely with parents/carers to ensure children are safe when using the internet, especially if there are concerns about the child's use of it that makes them particularly vulnerable.
Social workers may wish to discuss the level of supervision a child may need to keep them safe online and what practical actions parents/carers can take to improve internet safety. Such as use of filters and parental controls.
Information for parents/carers on e-safety can be found in the home's e-safety policy and resources folder.
Parents/carers need to know about the risks posed by ICT so that they can continue e-safety education at home and regulate and supervise children's use as appropriate to their age and understanding. Social workers should ensure that they have a copy of the CSF internet safety guide for parents/carers.

Parents use of the internet
Parents own use of the internet may raise concerns, for example, around accessing pornography on the internet. Where there is evidence that an adult in the household is viewing child sex abuse images, this will require a child protection response as it raises serious questions about the safety and welfare of children living in the household and who are in contact with the adult.
In such cases the matter will need to be dealt with by the Police and Social Services.

7. IT and Safe Working Practice

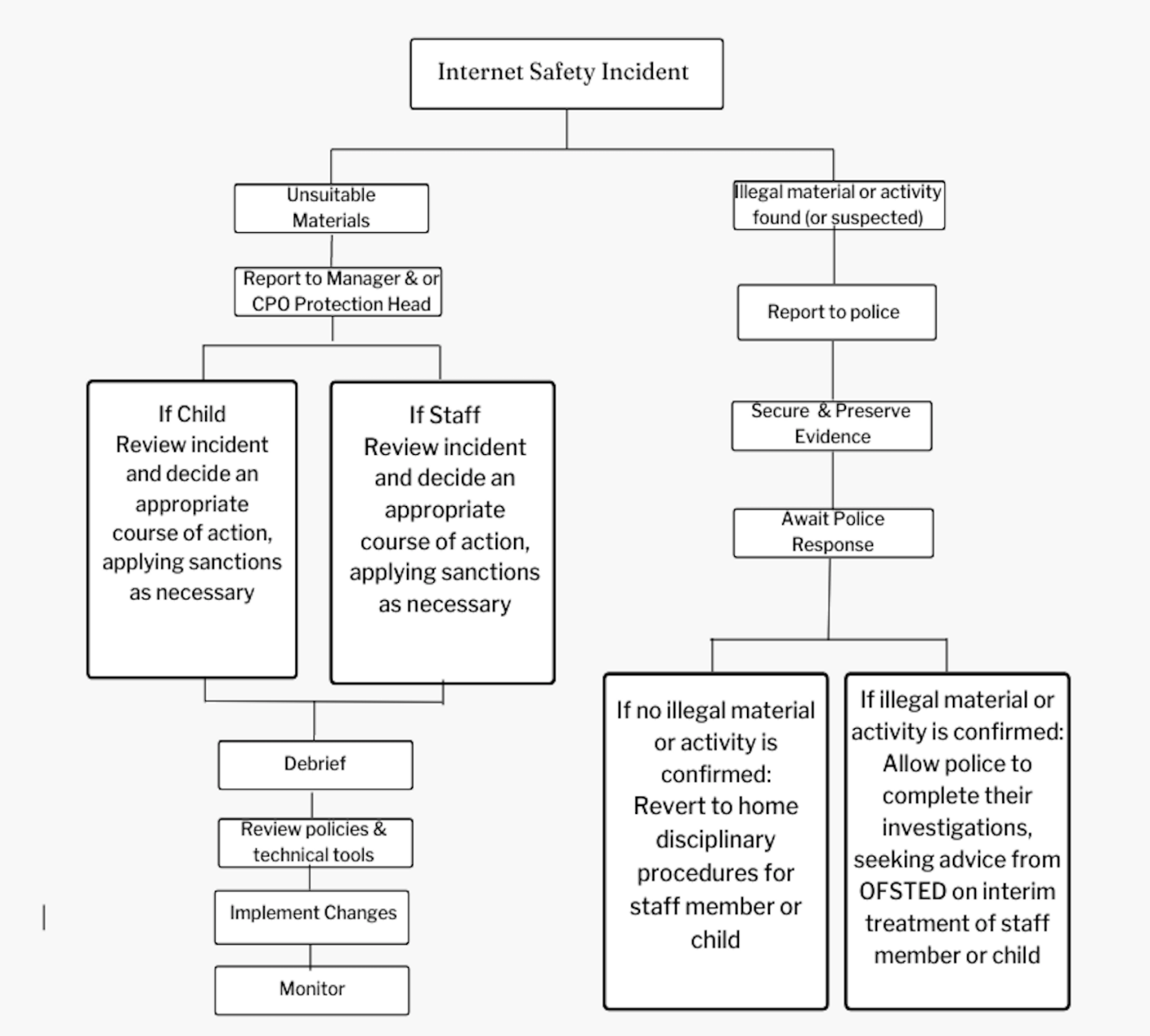
All professionals who work directly with children need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with children.
The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations:
Photographic and video images of children should only be taken as part of a clear work objective that has been agreed with managers and should be stored on work equipment.
Staff should only use work equipment and only store images on their work computer, with all other copies of the images erased.
Staff should take care regarding the content of and access of and access to their own social networking sites and ensure that children and parents/carers cannot gain access to these.
Staff should ensure that any materials published on their own social networking sites and neither inappropriate nor illegal and will not affect their professional standing or the integrity of the home.
Staff should not breach confidentiality by making any comments to do with specific children via the internet.
Staff should not breach confidentiality by making any comments to do with the home or other staff members via the internet.
Staff should not engage in any conversation with children via their private instant messaging or social networking sites as these may be misinterpreted or taken out of context.

When contacting children or parents by telephone, staff should avoid using their own phones. Children's or parent's/carer's numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to children.
Staff should ensure that personal data relating to children is stored securely and encrypted if taken out of the office.
Where staff members are using mobile equipment such as laptops provided by their employer, they should ensure that the equipment is always kept safe and secure.

All staff will be bound by their terms of employment and code of conduct, and these are likely to cover confidentiality and professional standards. Further, many members of the children's workforce will also be bound by professional rules regarding their conduct. Such rules are likely to cover use of the internet and it is recommended that all staff members are aware of any standards of behaviour expected from their employer or their professional body.

See also: Khaya Home Limited Safeguarding and Child Protection Policies and Procedures
Khaya Home Limited 'Code of Conduct for Staff'

Flowchart for responding to internet safety incidents in the home


Internet Safety Incident
Unsuitable Materials
Report to Manager & or CPO Protection Head
If Child Review incident and decide an appropriate course of action, applying sanctions as necessary
If Staff Review incident and decide an appropriate course of action, applying sanctions as necessary
Debrief
Review policies & technical tools
Implement Changes
Monitor
Illegal material or activity found (or suspected)
Report to police
Secure & Preserve Evidence
Await Police Response
If no illegal material or activity is confirmed: Revert to home disciplinary procedures for staff member or child
If illegal material or activity is confirmed: Allow police to complete their investigations, seeking advice from OFSTED on interim treatment of staff member or child