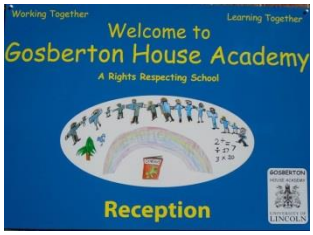


Gosberton House Academy

E-Safety Policy

Introduction

There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Gosberton House Academy has made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks."

However, Safeguarding is a serious matter; at Gosberton House Academy we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

This e-safety policy is an important part of our children's safeguarding and should be read in conjunction with other relevant policies such as behaviour, safeguarding and anti-bullying. This policy also incorporates an Acceptable Usage Policy that is signed by pupils and parents, as well as all staff.

Gosberton House Academy strives to put the UN Convention of the Rights of the Child at the heart of its curriculum. Within our community children's rights are actively taught, practised, respected, protected and promoted. Children's rights are promoted during all aspects of daily life.

This policy is not the sole responsibility of the ICT Subject Leader but is the responsibility of all staff and should be respected by all.

Aims

New technologies have 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 devices are powerful tools, which open up new opportunities for everyone. Children and young people should have an entitlement to safe Internet access at all times.

The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure the risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Gosberton House Website; upon review all members of staff will sign as read and understood both the *E-safety Policy* and *the Staff Acceptable Use Policy.* A letter will be sent home with students at the beginning of each school year.

Policy Governance (Roles and Responsibility)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology used within the school.
- Ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates in regards to training, identified risks and any incidents.

Principal

Reporting to the governing body, the Principal has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated jointly to the Health and Safety Officer and e-Safety Officer.

The Principal will ensure that:

- E-safety training throughout the school is planned and up to date and appropriate to the recipient.
- The designated e-Safety officer has had appropriate CPD in order to undertake the day to day duties
- All incidents are dealt with promptly and appropriately

e-Safety Officer

The day to day duty of e-Safety Officer is devolved to Vicky Edwards with joint support from the DPO Paul Squire.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise herself with the latest research and available resources for school and home use.

- Review the policy regularly and bring any matters to the attention of the Principal
- Advise the Principal, governing body on all e-safety matters
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the Local Authority, IT support and other agencies as required.
- Retain responsibility for the e-safety log; ensure staff know what to report and ensure the appropriate audit trail. [Kept in the cupboard in the ICT suite]
- Ensure any technical e-safety measures in school are fit for purpose through liaison with the LA/IT support.

IT Technical Support

Technical support staff [currently Ark] are responsible for ensuring that:

- Anti-virus is fit for purpose, up to date and applied to all capable devices.
- Windows and iOS updates are regularly monitored and devices updated as appropriate.
- E-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user.
- Passwords are applied correctly to all users as agreed by the Principal and e-Safety officer

All Staff

Staff are to ensure that:

- They have up to date awareness of e-safety matters, policies and practices.
- All details in this policy are understood. If anything is not understood it should be bought to the attention of the e-Safety Officer or Principal.
- Any e-safety incident is reported to the e-Safety Officer [and an e-safety incident report is made].
- The reporting flowcharts contained in this e-safety policy are fully understood.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school e-safety and acceptable use agreement.
- They monitor ICT activity in lessons and extra –curricular activities

Child protection Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

All Students

The boundaries of the use of ICT equipment and services in this school are given in the *Pupil Acceptable Use Policy*; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

[RRSA] Article 17: Every child has the right to reliable information from the mass media. Televisions, radio, newspapers and other media should provide information that children can understand. Adults must help protect children from materials that could harm them.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and the knowledge they need to ensure the safety of children outside the school environment. Through parents meeting, website and the school newsletter the school will keep the parents up to date with new and emerging e-safety risks, and will involve parents in strategies to provide a consistent approach.

Teaching and Learning

Why the Internet and digital communication are important

- An essential element to the 21st century life for education, business and social interaction. Therefore we have a duty to provide all our pupils with high-quality Internet access as part of their overall learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning

- Pupils will have clear boundaries for the appropriate use of the Internet and digital communication.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content

- Ensure the use of Internet materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they see and how to validate it.

Technology

Gosberton House Academy uses a range of devices including PCs, Laptop and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering: we use the Net Sweeper system that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites. The ICT Subject Leader, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are bought to the attention of the Principal.

Email Filtering: with google, there system prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script [malware] that could be damaging or destructive to data; spam email such as a phishing message.

https://support.google.com/a/answer/3292720?hl=en

Anti-Virus: all capable devices will have anti-virus software, monitored by Ark. This software will be updated regularly for new virus definitions. IT Support will be responsible for ensuring this task is carried out and will report to the Principal if there are any concerns. The anti-virus is AVG.

Passwords: all staff have their own personal passwords for the school network and email. These passwords are the responsibility of the staff to ensure that they are not compromised. They can be changed by the individual staff member. All classes have their own class logons to the school network and teachers teach this as appropriate to the individual needs of the children. The children do not have an email account. The iPads do not have a password but remain on school grounds; they are in the process of having a security setting [Lightspeed] on them which means they can be locked if they leave the school premises without permission.

Encryption: Laptops are set up so that the g:drive which hold important data is not available off the premises. After the broadband is upgraded we will be able to use the VPN system to access our secure server from home. We are currently looking at a phased upgrade to Windows 10 to allow all laptops to be encrypted.

Safe Use

Internet: use of the Internet in school is a responsibility, not a right. Internet use will be given to all staff and pupils upon signing the appropriate Acceptable Use Policies.

Email: emails are subject to Freedom of Information requests and as such the email service is to be used for professional work-based emails only. The children do not have an email address at school.

Photos and Videos: all parents must sign a photo/video release slip at the beginning of each academic year. Digital media such as photos and video should only be taken on school devices and stored on school equipment.

iPads can no longer be used as a toilet training aid.

Social Networking: there are many social networking services available; however at Gosberton House Academy we have decided that these are not appropriate for our children in light of their complex learning needs and vulnerability.

Our Health and Safety Officer has attended a Self-Harming / Bullying Workshop based on the effects of Social Media.

Incidents: any e-safety incident is to be bought to the immediate attention of the e-Safety Officer or the Principal. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of the Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer device connected to the school network.

Training and the Curriculum

It is important to Gosberton House Academy that staff and families feel empowered with the knowledge of staying safe and as risk free as possible, whilst using digital technology; this includes updated awareness of new / emerging issues and an annual training programme through *Educare.*

e-Safety for pupils is embedded into the curriculum both as part of Computing but also has cross curricular links to PSHE, social communication and our Rights and Responsibilities. Whenever ICT is used in school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the students learning. Staff have taken advantages of recommendations from the CEOP e-safety training in the past and use *Hector's World, Lee and Kim* and *Cyber Café,* resources are on the g;drive and within planning files. E-Safety is also included within the *Cornerstones ILP Curriculum.* Please read the Computing policy for more details about what is covered in the curriculum.

GDPR

Our GPO is Paul Squire, we are working on a phased programme of converting laptops to Windows 10 to be able to encrypt devices. We are looking at upgrading the server to allow RDA access for teaching staff, we currently use VPN.

GDPR is a work in progress. Staff have had initial training via Educare and an information meeting. They are aware not to take sensitive data off the premises on the desktop or via hard drives.

iPads do not contain any personal data.

Review Date: September 2019

Gosberton House Academy

Staff Acceptable Use Policy

Note: all Internet and email activity is subject to monitoring

You must read this in conjunction with the *e-Safety Policy.* Once you have read and understood both you must sign the Staff Agreement sheet.

Internet access: you must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident and reported to the e-Safety Officer and an incident sheet completed.

Social Networking: is not allowed in school. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks.

Use of email: staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords: staff should keep passwords private.

Data Protection: if it is necessary to take work home, or off site, you should ensure that your device is encrypted.

Personal Use of School ICT: you are not permitted to use ICT equipment for personal use unless specific permission has been given by the Principal. Equipment being used away from school for school use needs to be signed out of the specific book in the Principal's office.

Images and Videos: you should not upload onto any internet site, service or personal device.

Use of personal ICT: use of personal ICT equipment is at the discretion of the Principal. Permission must be sought stating the reason for using personal equipment.

Virus and other Malware: any virus outbreaks are to be reported to the Ark helpdesk as soon as it is practical to do so.

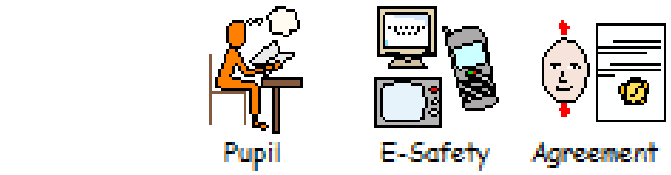
e-safety: like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT.

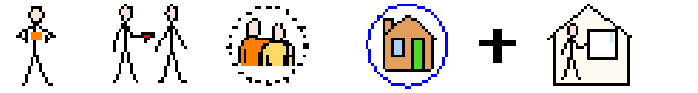
Dated: September 2019

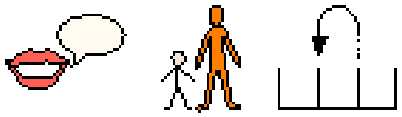
Gosberton House Academy

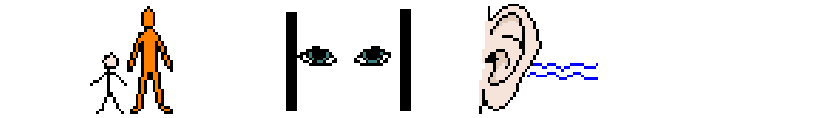
Pupil Acceptable Use Policy

Charter of Good Online Behaviour

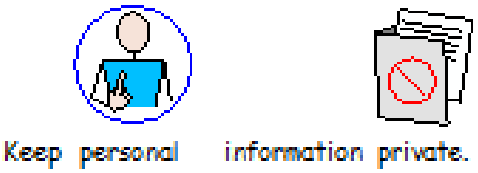








worries you.



Class _____

Why we Filter the Internet

[taken from SafeICT]

Introduction

Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the e-safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects:

Very broadly speaking

- Filtering - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- Monitoring - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

Why do we Filter and Monitor?

Schools filter Internet activity for two reasons:

We filter to ensure

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

A right to privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this guide, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

Managing Expectations

It is the expectations of the user that is particularly important; this will include school staff, students and parents/guardians of the students. Consent is not a requirement, however you are required by law (Data Protection Act 1998) to make all reasonable efforts to inform users that you are monitoring them. By making reasonable efforts you are working "with" the students and parents, not just merely telling them.

Explaining to parents, staff and students

As previously mentioned, it is the understanding that is important, not the consent. It is not appropriate to simply have a sentence in the school e-Safety or Acceptable Use Policy and for that to suffice; privacy is always an emotive issue.

Here are the "must do's":

- Statement in e-Safety Policy,
- Statement in Acceptable Use Policy,
- Explain to staff why monitoring is important, allow them to voice any concerns and set their expectations of how the data can be used.
- Explain to the students as well, allow them to ask questions.
- A letter home to parents, again explaining that the Internet activity may be monitored, and why. Assure the parents that you talk to the students, who are allowed to voice concerns and ask questions. This letter forms part of the term 1 paperwork; including the Acceptable Use Policy and a signature sheet. Parents (and students if old enough) should sign the letter to say they understand, not to agree as again, consent is not required.
- A questionnaire to go home at the same time to gauge parental voice (see g;drive and website]) [Don't forget, Ofsted require that schools engage with parents and students when creating policy.]

Summary

- Filtering is different to monitoring.
- You do not require consent.
- But you must tell users if you do monitor, or if you have the facility to monitor.
- Set user expectations; explain under what circumstances it may be a requirement to monitor.
- Ensure you have a good statement in your e-Safety Policy.
- Ensure you have informed users that Internet use "May be subject to monitoring" in your Acceptable Use Policy.
- Ensure parents are informed, the reason why monitoring may take place, and they sign as read and understood.

Draft letter to parents

Dear Parent /Guardian

Use of the Internet at Gosberton House Academy is a vital part of the education of your son/daughter. Our school makes use of the Internet in order to enhance their learning and provide facilities for research.

You will be aware that the Internet is host to a great many inappropriate sites and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this through Internet filtering. This filter categorizes websites in accordance with their content; the school allows or denies these categories upon agreement by the IT Support provider and ourselves.

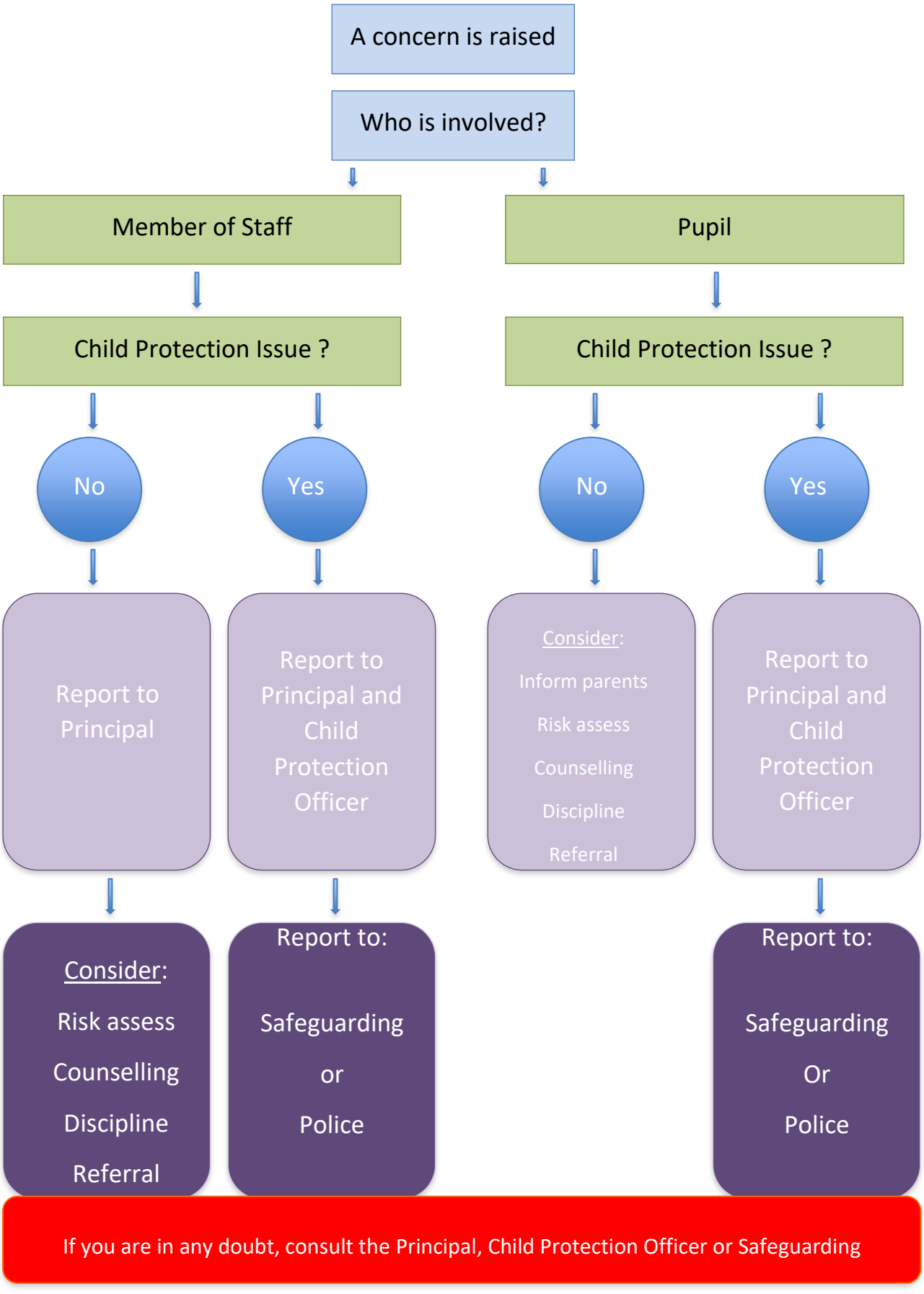
Security and Safeguarding of your child are of the upmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor internet logs. We will inform you immediately if we believe your child has been involved in any questionable activity.

We address aspects of e-Safety with your child as part of their Curriculum. We would highly recommend that you also spend time with your child to transfer this important knowledge and to help support them to keep themselves safe.

Yours Sincerely

Vicky Edwards

Inappropriate Activity Flowchart



Illegal Activity Flowchart