L.E.A.D. Academy Trust

Lead • Empower • Achieve • Drive

E-Safety Policy

WITHAM ST HUGHS ACADEMY

POLICY DOCUMENT: *E-SAFETY*

Introduction

The use of digital technology is now seen as an essential part of everyday life and Witham St Hughs Academy recognise that the internet and other digital technologies provide a good opportunity for children to learn. The number of SMS (text) messages and emails sent everyday greatly exceed the population of the planet. Nearly every company, organisation, agency, school and local authority has a presence somewhere on the internet, allowing them to engage a variety of people in different ways.

Our academy's policy is aimed at providing a balance between exploring educational potential and new technologies whilst safeguarding pupils. By reviewing our E-safety policy and procedures we are able to ensure that technology and the internet has a positive impact on children's learning and understanding. We use the opinions and knowledge of the children to assist us with developing E-safety within our academy.

While digital technology can be used in positive ways to develop and promote creativity, stimulate awareness and enhance learning, it can also be used in extremely negative ways. Paedophiles use this technology to contact, groom and blackmail young people in the virtual world with a view to abusing them in the real world, children and young people are able to anonymously bully classmates and teachers, known as cyber-bullying, while adults may find themselves at greater risk of identity theft should they publish too much information about their life onto a social network.

The risks are real but many people do not see that activity within a virtual world can have an effect in the real world. Comments posted onto social networking sites have led to staff being disciplined and young people being bullied. Many are also unaware of legal ages for some online activities and that in the virtual world this misuse of the internet can lead to criminal offences and prosecution.

The Lincolnshire Safeguarding Children Board has overall statutory responsibility for the safeguarding of the child, and that includes the virtual world as well as the real, and takes seriously the role it has to en- sure that member agencies co-operate to safeguard and promote the welfare of children and young people in the locality, and to ensure that they are effective in doing so.

Policy Statement

Primarily e-Safety is used to describe pro-active methods of educating and safeguarding children and young people while they use digital technology. In order for children and young people to re- main safe we should educate them not only in the dangers but also inform them who they can contact should they feel at risk and where to go for advice while still promoting the many benefits of using digital technology, thereby empowering them with the knowledge and confidence of well researched, good practice and continuing development.

The large majority of reported incidents involve children being contacted by adults for sexual purposes, visiting highly inappropriate websites or being bullied by their peers through technology. However, it should also be remembered that there have been instances where adults have been the victims through a lack of knowledge of the dangers present and by not applying real world common sense to the vast virtual world available to them on the internet.

The objective of this policy is to state a minimum standard required by Lincolnshire County Council so that schools and other establishments in Lincolnshire can build their own requirements based on own needs.

This policy applies to all pupils, all teaching and support staff, school governors, volunteers and all aspects of the school's facilities where they are used by volunteers and community organisations.
Witham St Hughs Academy will ensure that the following elements are in place as part of its safeguarding responsibility to pupils:

- Information to parents that highlights safe practice for children and young people.
- An updated E-safety policy.
- Information to parents and young people about new technology used in school.
- Training for all staff.
- Close supervision of pupils when using technology.
- Education that is aimed at ensuring safe and responsible use of new technology.

What is E-Safety
Within Lincolnshire, the definition of e-safety is the proactive and reactive measures to ensure the safety of the child, and adults working with the child, whilst using digital technologies. This extends to policy, training and guidance on the issues which surround risky behaviours, and encompasses the technical solutions which provide further safeguarding tools. It should be remembered that digital technology reaches far and wide, not only computers and laptops, but consideration should also be given to technologies such as: iPads, iPod Touches and iPhones; Xbox; Playstations; Wii; mobile phones and PDA's, and anything else which allows interactive digital communication.

- E-safety concerns safeguarding children and young people in the digital world.
- E-safety emphasises learning to understand and use new technologies in a positive way.
- E-safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- E-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

The Internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networks all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Some of the material on the Internet is published for an adult audience and can include violent and adult content. Information on weapons, crime and racism may also be unsuitable for children and young people to access. Pupils and staff need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Schools have a duty of care to enable pupils to use on-line systems safely. Schools need to protect themselves from legal challenge and ensure that staff work within the boundaries of professional behaviour. The law is catching up with Internet developments: for example, it is an offence to store images showing child abuse and to use email, text or instant messaging (IM) to 'groom' children.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised" and ensure an Acceptable Use Policy is in place. E-Safety training is an essential element of staff induction and part of an ongoing CPD programme. However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

The rapid development and accessibility of the Internet and new technologies such as personal publishing and social networking means that e-Safety is an ever growing and changing area of interest and concern. The school's e-Safety policy must reflect this by keeping abreast of the vast changes taking place around us. At this school, e-safety awareness is built into the curriculum around the areas grouped as 'the 4 C's', which are as follows:

Content	**Contact**
Unsuitable or potentially illegal material, including offensive or pirated content	Unwelcome or inappropriate contact, such as grooming or sexual contact
Conduct	**Commerce**
Behaviour (as a recipient or active participant), includes bullying or giving out too much personal info	Actions with a financial or commercial consequence, from phishing or identity theft

The academy's e-Safety Policy operates in conjunction with other policies including Behaviour, Child Protection and Anti-Bullying.

Use of New Technologies

Witham St Hughs Academy seeks to safeguard pupils and staff whilst using new technologies effectively for their intended educational purpose, ensuring there is no infringing of legal requirements or creating unnecessary risk. Our academy expects staff and pupils to use new technology for an educational purpose only and must strictly follow the conditions below whilst using the internet and new technologies. These expectations also apply to volunteers and community organisations that may use Witham St Hughs Academy's ICT facilities and digital technologies:

- ➢ Visit internet sites to make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to the following:
  - Indecent images of children
  - Promoting discrimination of any kind
  - Promoting racial or religious hatred
  - Promoting illegal acts
  - Share private/personal information about pupils, staff, volunteers or Witham St Hughs Academy
  - Any information which could be deemed offensive or upsetting (cyberbullying)

Witham St Hughs Academy understands that some websites or technologies that may be deemed as inappropriate may be beneficial for education use. In this instance, access must be pre-planned and recorded and permission given by Senior Leaders and L.E.A.D ICT technicians.
Monitoring safe use of new technologies includes both personal use of the Internet and electronic mail. Staff should monitor patterns and trends of new technologies. Staff will investigate the use of new technologies used by pupils particularly where these technologies may be used to cause harm to others, e.g. cyber bullying. Where necessary, staff will support individual pupils where they have been deliberately or inadvertently been subject to harm.

Working in Partnership with Parents

Witham St Hughs Academy are committed to working with parents and carers and understand the key roles they play in maintaining the safety of their children, through promoting internet safety at home and the use of safe and appropriate use of new technologies.

Cyber Bullying

Cyber bullying is the sending or posting of harmful or cruel text or images using the Internet or other digital communication devices. 33% of children have been bullied online but only 4% of parents know this. It is clear that Cyberbullying is on the increase and it tends to happen more outside of school than in school, on a range of new technologies. Phone calls/ text message and email are the most common forms of cyberbullying.

Examples of cyber bullying which distinguishes it from other forms of bullying include:

- **Flaming**: Cyber bullying insults can get angrier and more vulgar. The indirect and often anonymous nature of it makes the bully more likely to escalate what they say and threaten.
- **Harassment**: The ease of communications results in anonymous taunts, insults, and threats which are ongoing and frequent in nature.
- **Denigration**: This is where the bully sets up a false profile with cruel and false contents and posts further vulgar information. It is difficult to pretend to be someone else in the real world.
- **Impersonation**: This is the stealing of passwords to send threatening messages including breaking into an e-mail account and sending vicious or embarrassing material to others pretending it is from someone else.
- **Outing**: This is the sending of intimate personal information to others (covert photos) for example taking a picture of a person in the locker room using a digital phone camera and sending that picture to others.
- **Exclusion**: This is ex-communication of an individual from "buddy lists" which leads to real cruelty as the person affected feels isolated and excluded.
- **Cyber Stalking**: This is blackmail (from photos) and sending of harmful messages.
- **Cyber Threats**: Direct or actual threats to hurt or commit suicide.

Often young people report that cyber bullying starts as a prank, but due to the anonymity and indirect nature of cyber bullying, there tends to be a lack of empathy with the victim leading to escalation.
The impact of cyber bullying is different to bullying in the real world, in that there is no escape. If a young person is being bullied at school, they may feel safe at home, whereas mobile phone access / technologies can be accessed 24 hours a day, 7 days a week.

Witham St Hughs Academy will follow these steps if cyberbullying is reported or suspected within the academy:

- Preserve the evidence of cyberbullying.

- Encouraged pupils to 'Block' and report the user to the service provider.

- Death threats or threats of other forms of violence to a person or property, any evidence of sexual exploitation is illegal and will be reported to the police.

- Assist with parents understanding of cyberbullying and recommend steps to follow at home to reduce cyberbullying.

The following is a minimum requirement to which all academy staff should adhere

E-Safety Policy: Staff

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 other information which may be illegal or offensive to colleagues.

It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student access any of these sites unintentionally you should report the matter to a member of the Leadership Team so that it can be logged.

Access to any of the following should be reported to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

Social Networking – Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available.

Members of staff should never knowingly become "friends" with students on any social networking site or engage with pupils on internet chat. Caution should be exercised in accepting 'friends' who are parents of children attending the academy. All information published on social media should be able to stand up to public scrutiny should the content be challenged. Any published information that could reflect negatively on the academy or any individual within it, could result in disciplinary action being taken against members of staff. This includes photographs or comments which could be interpreted by others as bringing the academy's integrity into question.

Use of Email - All members of staff should use their professional email address for conducting academy business. Use of academy email for personal/social use is at the discretion of the Headteacher.

Passwords - Staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced.

Personal Use - Staff are permitted to use ICT equipment for personal use within the guidelines contained in this policy.

Images and Videos - Staff and pupils should not upload onto any internet site images or videos of themselves or other staff or pupils without consent, and should never uploads content which could damage the reputation of the academy.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the academy. Any such use should be stringently checked for up to date anti-virus and malware checkers.

Viruses and Other Malware - any virus outbreaks are to be reported to ACS as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the academy.

Staff should note that internet and email may be subject to monitoring

E-Safety Policy: Pupils

The use of ICT within schools has enormous benefits to education, however there are reasons why the school and the local authority must put some restrictions in place, such as: ICT equipment is very expensive to buy and maintain; the school and the local authority have a duty of care to ensure that pupils are safe and not exposed to illegal or inappropriate content. It is hoped that these restrictions do not interfere with pupil education, but if pupils feel otherwise they should talk to a member of staff to discuss any issues.

Use of the Internet - the internet is provided to help you with learning activities such as research, online activities, online educational games and many other things. The internet is not to be used to access any- thing which is illegal, or anything that someone else may find offensive. This would include pornography, discrimination, racial or religious hatred. If you are unsure, or if you come across anything you feel is inappropriate, you should turn your computer monitor off and let your teacher know. Never try to bypass the security by using proxy sites, these are all monitored.

Logins and Passwords - every person has a different computer login and password. You should never allow anyone else to use your details. If you think someone else may have your details you should have your password changed.

User Areas - your user area is provided for you to save school work. It is not to be used to save music or other files that you have brought in from home.

Social Networking - if social networking (for example Facebook, Twitter) is allowed in the academy you should never upload pictures or videos of others without their permission. It is not advisable to upload pictures or videos of yourself, videos and pictures can easily be manipulated and used against you. You should never make negative remarks about the academy or anyone within the academy. Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc. Consider using a nickname and only inviting people you know. Universities and future employers have been known to search social networking sites.

Beware of fake profiles and people pretending to be somebody else. If something doesn't feel right follow your instincts and report it to an appropriate adult. Never create a false profile as a joke and pretend to be somebody else. This can have serious consequences.

Some social networking sites have a chat facility. You should never chat to anyone that you don't know or don't recognise. It is recommended that you never meet a stranger after meeting them online. If you do, always inform your parents and take one of them with you.

Cyber Bullying – you should not send harmful, personal or cruel text or images, whilst suing the internet and new technologies.

Security - you should never try to bypass any of the security in place, this includes using proxy bypass sites. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts.

Copyright - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that it is owned by somebody else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Etiquette - many schools provide students with email accounts, or let students post on things like blogs. Always be polite and don't swear. Consider what you are saying, and how it might be read by somebody else. Without emoticons it is difficult to show emotions in things like emails and blogs, and some things you write may be read incorrectly.

Mobile Phones - Some modern mobile phones offer the same services as a computer, i.e. Facebook, YouTube, email access etc. This can be a great way of keeping in touch with your friends and family. But, in the same way that some internet services can be used inappropriately, the same is true with mobile phones.

Never take inappropriate pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else. In some circum- stances this can be an illegal act.

Useful Websites

CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an ex- cellent educational programme, as well as advice and videos for all ages on their website.
www.ceop.gov.uk

IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content.
www.iwf.org.uk

BBC - a fantastic resource of e-safety information for the younger child.
www.bbc.co.uk/cbbc/help/web/staysafe

Cybermentors is all about young people helping and supporting people online.
www.cybermentors.org.uk

Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same.
www.digizen.org

Some Simple Do's And Don'ts For Everybody

- Never give out personal details to online friends that you don't know offline.

- Understand what information is personal: i.e. email address, mobile number, school name, sports club, meeting up arrangements, pictures or videos of yourself, friends or family. Small pieces of information can easily be pieced together to form a comprehensive insight into your personal life and daily activities.

- Think carefully about the information and pictures you post on your profiles. Once published online, anyone can change or share these images.

- It can be easy to forget that the internet is not a private space, and as result sometimes people engage in risky behaviour online. Don't post any pictures, videos or information on your profiles, or in chat rooms, that you would not want a parent or carer to see.

- If you receive spam or junk email and texts, never believe the content, reply to them or use them.

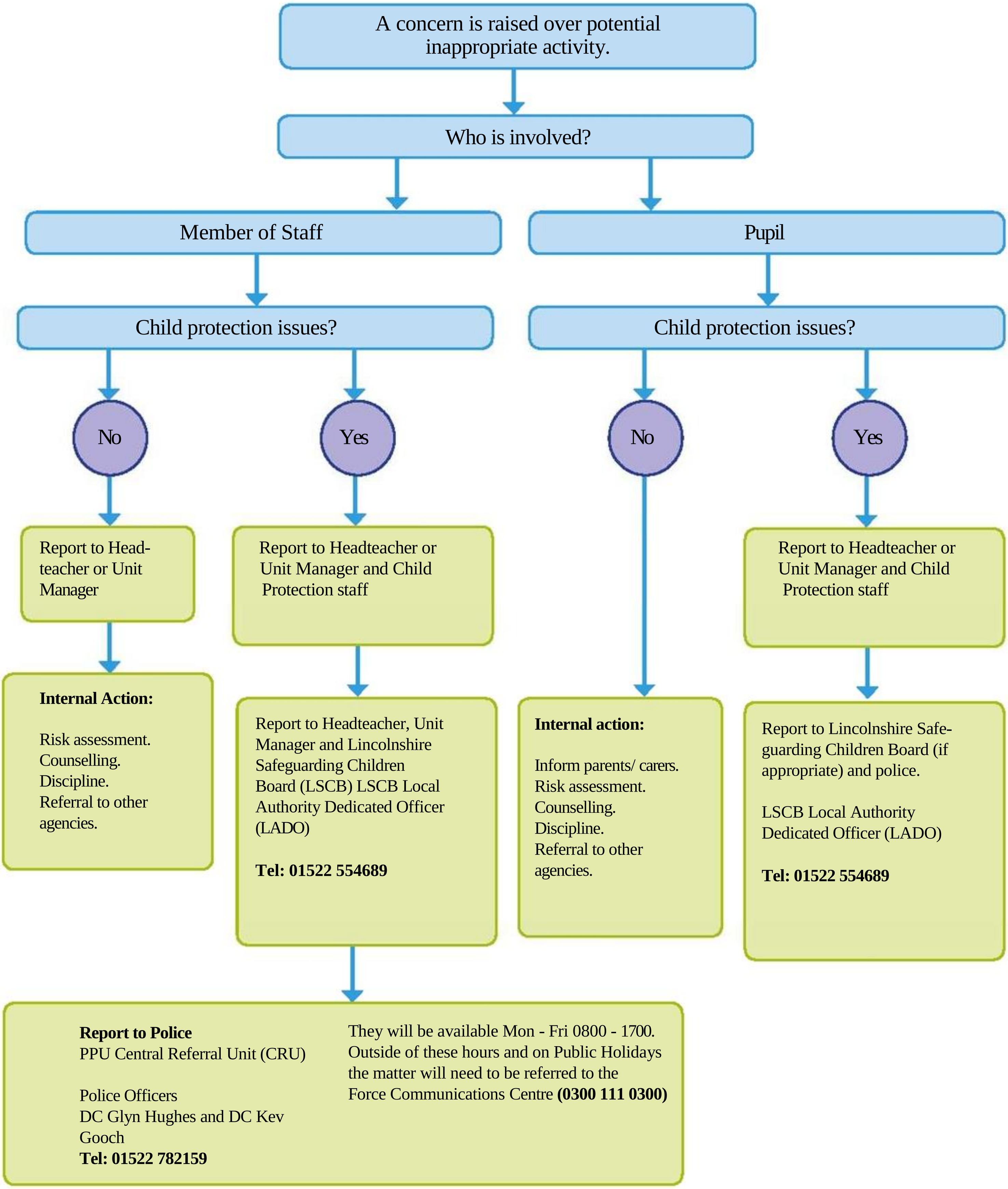
- Don't open files that are from people you don't know. You won't know what they contain - it could be a virus, or worse - an inappropriate image or film.

- Understand that some people lie online and that therefore it's better to keep online mates online. Never meet up with any strangers without an adult that you trust.

Don't forget, it is never too late to tell someone if something or someone makes you feel uncomfortable.

Policy Last Reviewed : April 2019

Inappropriate Activity flowchart



A concern is raised over potential inappropriate activity.

Who is involved?

Member of Staff

Child protection issues?

No

Report to Head-teacher or Unit Manager

Internal Action:

Risk assessment.
Counselling.
Discipline.
Referral to other agencies.

Yes

Report to Headteacher or Unit Manager and Child Protection staff

Report to Headteacher, Unit Manager and Lincolnshire Safeguarding Children Board (LSCB) LSCB Local Authority Dedicated Officer (LADO)

Tel: 01522 554689

Report to Police
PPU Central Referral Unit (CRU)

Police Officers
DC Glyn Hughes and DC Kev Gooch
Tel: 01522 782159

They will be available Mon - Fri 0800 - 1700. Outside of these hours and on Public Holidays the matter will need to be referred to the Force Communications Centre **(0300 111 0300)**

Pupil

Child protection issues?

No

Internal action:

Inform parents/ carers.
Risk assessment.
Counselling.
Discipline.
Referral to other agencies.

Yes

Report to Headteacher or Unit Manager and Child Protection staff

Report to Lincolnshire Safe-guarding Children Board (if appropriate) and police.

LSCB Local Authority Dedicated Officer (LADO)

Tel: 01522 554689