Thurlby Community Primary School
Acceptable Use of ICT Policy

This policy has been created using the e-safety policy of Lincolnshire Safeguarding Children's Board and the Acceptable Use of ICT Policy (AUP).

Our School e-Safety Policy reflects the importance we place on the safe use of information systems and electronic communications.

The school policy for Acceptable Use of ICT reflects the consensus of opinion of the whole teaching staff. It has been drawn up as a result of staff discussions and has the full agreement of the Governing Body.

It was agreed at the 26th January 2016 meeting of the Governing Body.

The implementation of this policy is the responsibility of all the teaching staff.

Definition of 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 360; Playstations; Nintendo Wii; mobile phones and PDA's, and anything else which allows interactive digital communication.

Our e-Safety Aims

We aim to:

- safeguard children and young people in the digital world
- emphasise learning to understand and use new technologies in a positive way
- develop an ethos, less about restriction and more about education allowing children to be confident online by teaching about the risks as well as the benefits
- support children to develop safer online behaviours both in and out of school.

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.

Our e-Safety policy must reflect this by keeping abreast of the vast changes taking place around us. With this in mind, the policy will be reviewed every year.

Our e-Safety Policy operates in conjunction with our Behaviour (including Anti-Bullying) and Child Protection policies.

E-safety is a vital part of our PSHE curriculum.

Managing Whole School Access to the Internet

To provide assistance in safeguarding we use Internet filtering.

Inappropriate content and sites are blocked. If a teacher needs to site unblocking, they will need to speak to the Headteacher who will discuss the matter with Ark ICT Solutions technicians in good time and be able to explain how the site is going to be used and how children will be protected. A decision whether to unblock a site will then be made.

Ultimate responsibility for e-safety lies with the Head teacher and Senior Leaders. Safeguarding decisions must be made by them.

Staff Development (CPD)

All staff on starting, will be made aware of e-safety as part of the safeguarding induction.

E-safety training and awareness sessions will be made available for staff, students and parents each year. This may be in-house training, provided by the Police/PCSO or from an outside agency.

Ark IT solutions will keep up to date with developments in technology and the consequent risks it involves.

Responsibilities of School Staff & Governors

If staff require it, further advice can be sought from Lincolnshire Safeguarding including Lincolnshire’s E-safety officer, Dan Hawbrook (dan.hawbrook@lincolnshire.gov.uk).

All staff will receive a copy of this policy on appointment.

Staff must be aware that the school can monitor network and Internet usage to help ensure staff and pupil safety.

The procedures defining how inappropriate or illegal ICT use is reported are included in Appendices 1 & 2.

Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source.

Email, text messaging, Social Networking and Instant Messaging (IM) all provide additional channels of communication between staff and pupils. Inappropriate behaviour can occur and communications can be misinterpreted. Staff should be aware of the power of the Police to identify the sender of inappropriate messages.

Schools provides establishment email accounts for all staff.

Staff should be aware that children may be subject to cyberbullying via electronic methods of communication both in and out of schools. Head teachers should be aware that they have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site (Education and Inspections Act 2006).

School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school Behaviour Policy (Education and Inspections Act 2006).

Any allegation of inappropriate behaviour must be reported to the Senior Leadership Team and investigated with care.

If there is any suspicion of illegal activity staff should NEVER investigate themselves but must report to Lincolnshire Police as soon as possible.

E-Safety Guidelines for Staff & Governors

Internet access - staff 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 Senior Management 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 – sites are blocked in school.

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.

Staff and Governors should not use social networking sites to comment on school life or issues.

Use of Email - all members of staff should use their professional email address for conducting school business. Use of school email for personal/social use is not permitted.

Passwords - staff should keep passwords private. Passwords are confidential and individualised to each person. Passwords should be alpha-numeric to give greater protection.

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. USB memory sticks should be encrypted, as they can be easily misplaced. Laptops should be protected with passwords.

File sharing - technology such as peer to peer (P2P) and bit torrents is not permitted on the Lincolnshire School's Network.

Personal Use - staff are not permitted to use ICT equipment for personal use.

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.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the school. Any such use will be stringently checked for up to date anti-virus and malware checkers. Our IT system has protection against unknown equipment trying to access it.

Viruses and other malware - any virus outbreaks are to be reported to the Ark Solutions technicians and the Headteacher as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Staff should note that Internet and email may be subject to monitoring.

E-Safety for Pupils

Pupils will be encouraged to talk to a member of staff to discuss any issues they have with esafety. A list of Child Exploitation and Online Protection (CEOP) Dos and Don'ts is included as Appendix 3.

E-safety will be taught primarily through the PSHE curriculum during every school year. This is supplemented with the computing curriculum and when the children are using ICT in other subjects too. E-safety and cyber-bullying will also feature heavily during anti-bullying week each year.

During e-safety lessons, children will be taught:

- that Internet and email use may be subject to monitoring
- that they will be allowed to access the Internet for learning activities such as research, online activities and online educational games but that the Internet is not to be used to access anything which is illegal, or anything that someone else may find offensive
- if children are unsure about something they see on the Internet, or if they feel something is inappropriate, to close the page and let their teacher know
- to never try to bypass the security by using proxy sites, as these are all monitored. This security is in place to protect them from illegal sites, and to stop others from hacking into other people's accounts
- that they should never allow anyone else to know and use their logins or passwords. If they think someone else may have their details they need to tell a member of staff
- that social networking (for example Bebo, Facebook, Flickr) is not allowed in school
- that they should never upload pictures or videos of other people
- that it is not advisable to upload pictures or videos of yourself
- the seriousness of making negative remarks about the school or anyone within the school
- when using social networks, to 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.

- when using social networks, to consider using a nickname and only inviting people you know.
- when using social networks, to beware of fake profiles and people pretending to be somebody else. If something doesn't feel right to follow their instincts and report it to an appropriate adult. They will be taught to never create a false profile as a joke and pretend to be somebody else, as this can have serious consequences
- to never use an instant chat facility to chat to anyone that you don't know or don't recognise. It is recommended that they never meet a stranger after meeting them online. If they do, they should inform their parents and take one of them with them
- that 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 they are unsure, they should ask a teacher
- when using school email, to always be polite
- that in the same way that some Internet services can be used inappropriately, the same is true with mobile phones
- children are not permitted to bring mobile phones into school, if they find their phone at school they shall be handed in to the Office or class teacher for safe keeping.

Review

The Headteacher and staff will review this policy in the Spring term. Any suggested amendments will be presented to the Governors for discussion at the meeting in the Spring 2017.

Useful websites:

CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. www.ceop.gov.uk

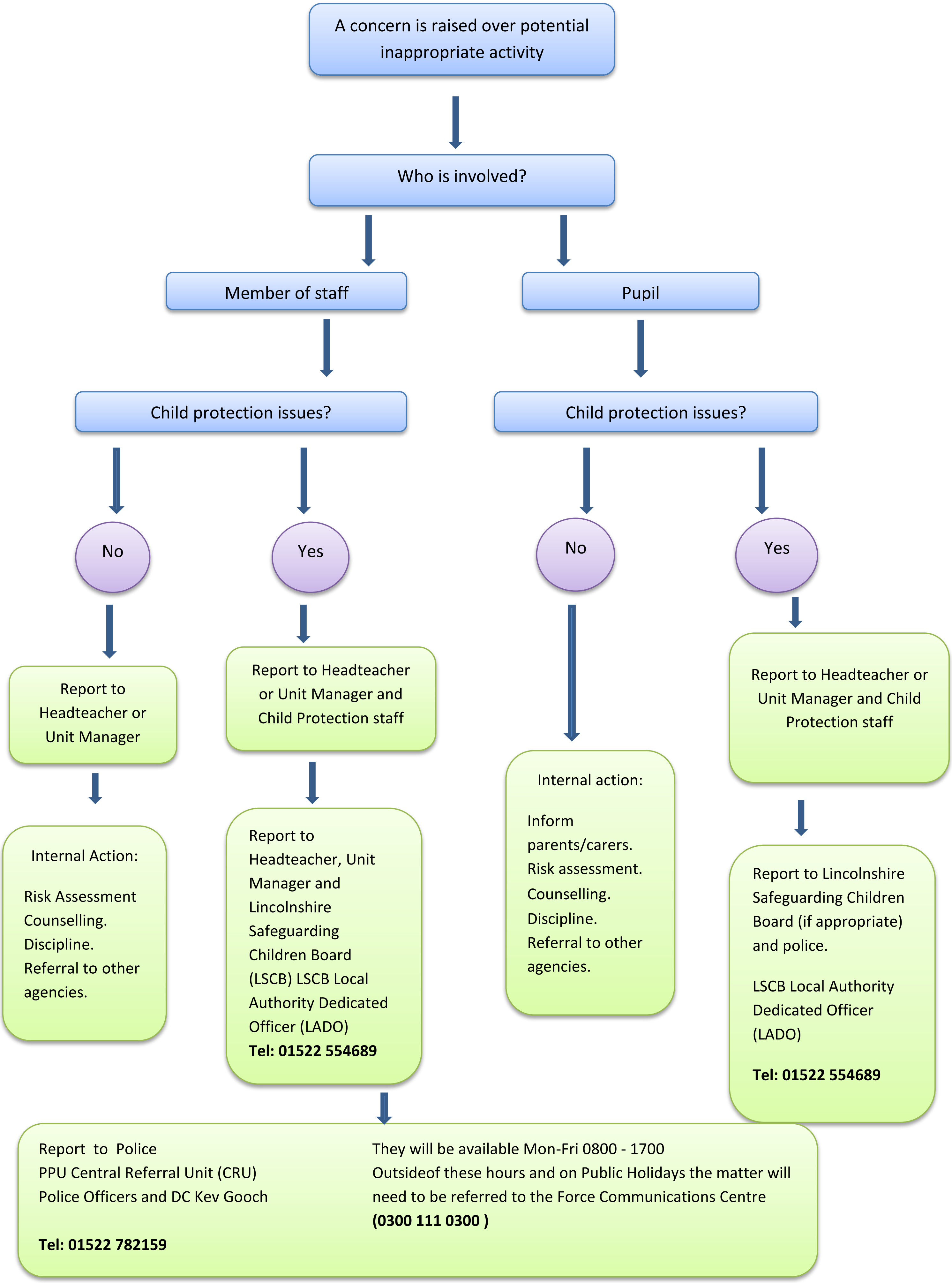
IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content. www.iwf.org.uk

BBC - 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

Appendix 1 Inappropriate Activity flowchart



A concern is raised over potential inappropriate activity

Who is involved?

Member of staff

Child protection issues?

No

Report to Headteacher 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

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 Safeguarding Children Board (if appropriate) and police.

LSCB Local Authority Dedicated Officer (LADO)

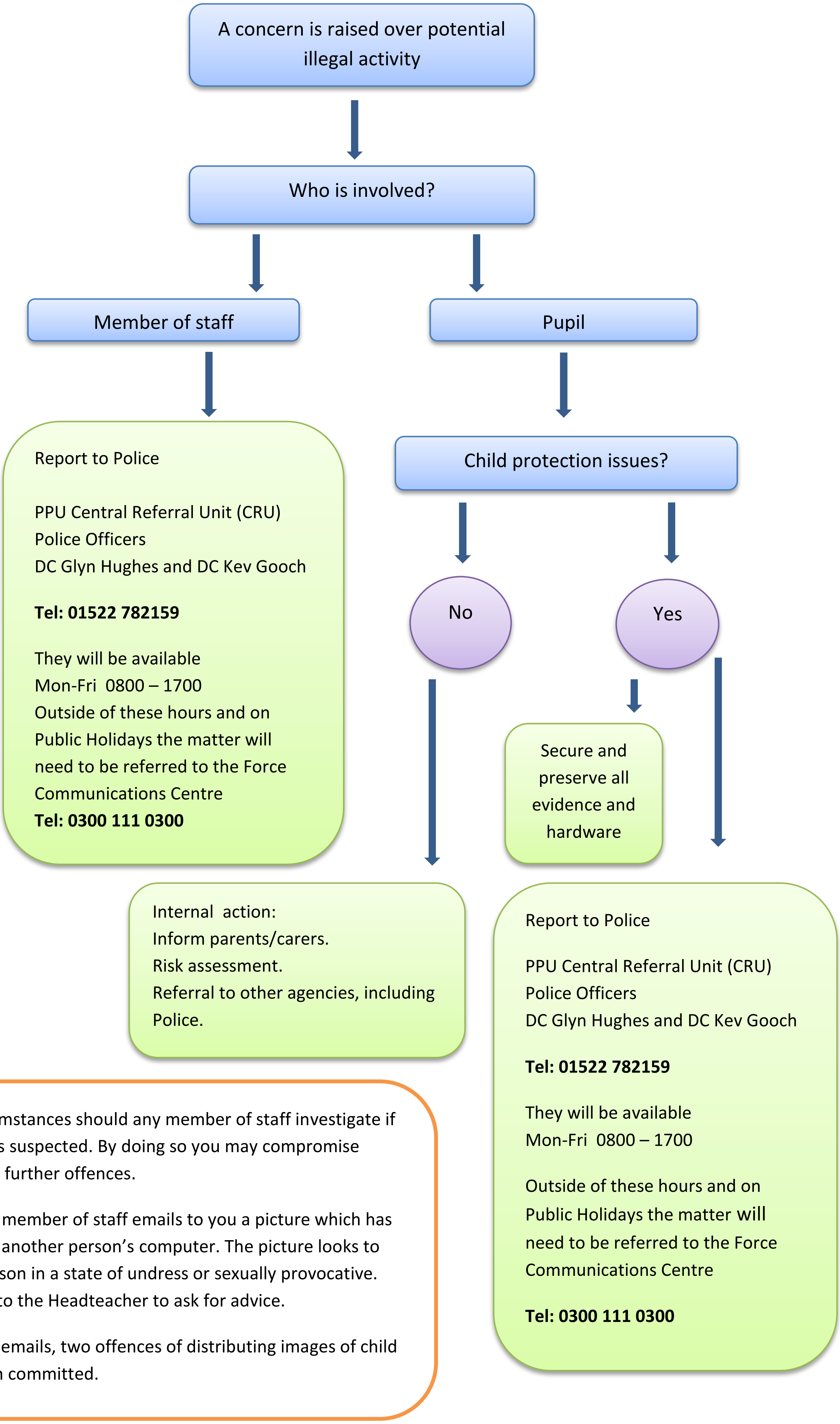
Tel: 01522 554689

Report to Police
PPU Central Referral Unit (CRU)
Police Officers and DC Kev Gooch

Tel: 01522 782159

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

Appendix 2 Illegal Activity flowchart



A concern is raised over potential illegal activity

Who is involved?

Member of staff

Pupil

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
Tel: 0300 111 0300

Child protection issues?

No

Yes

Secure and preserve all evidence and hardware

Internal action:
Inform parents/carers.
Risk assessment.
Referral to other agencies, including Police.

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

Tel: 0300 111 0300

Under no circumstances should any member of staff investigate if illegal activity is suspected. By doing so you may compromise and/or commit further offences.

For example, a member of staff emails to you a picture which has been found on another person's computer. The picture looks to be a young person in a state of undress or sexually provocative. You email this to the Headteacher to ask for advice.

Within these 2 emails, two offences of distributing images of child abuse has been committed.

Appendix 3

Dos and Don’ts

Some simple dos and don’ts for everybody (courtesy of CEOP):-

- 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 a 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.