Bicker Preparatory School and Early Years

E-Safety & Acceptable Use Policy

ICT and Computing Policy

Social Networking 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.

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) Prevent 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 provided externally by ARK ICT.

Inappropriate content and sites are blocked. If a teacher needs a site unblocking, they are able to access the site on their personal laptop via a proxy switch. If a teacher requires a site to be 'un-blocked' on the children's hardware, then a request has to be put to the Management Team and a request is then presented to ARK ICT.

Our IT system actively monitors Internet use and the Management Team are notified of any attempts to access inappropriate sites. These attempts are followed up by the Management Team and Class Teacher.

At present, computer tablets in school are also filtered by ARK ICT.

Ultimate responsibility for e-safety lies with the Head teacher and Management Team. 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 such as theatre group or Lincolnshire Safeguarding Officer or Stay Safe Partnership.

The IT Coordinator and Management Team will keep up to date with developments in technology and the consequent risks it involves.

Responsibilities of School Staff

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 Internet usage to help ensure staff and pupil safety.

Staff that manage filtering systems or monitor ICT use have great responsibility and must be appropriately supported.

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 and staff should therefore only contact children and families via accepted channels. This includes the school email account and landline telephone. Mobile phones should only be used in exceptional circumstances eg. When on school trips. At all other times, mobile phones should be left in the school office. Staff should be aware of the power of the Police to identify the sender of inappropriate messages.

Schools provides an establishment email account for all staff to use for school related emails.

Staff should be aware that students 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).

Children are discouraged from bringing mobile phones into school. Those that do know that their phones must be placed in the basket in the office.

Any allegation of inappropriate behaviour must be reported to the Management 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

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 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. We would expect that our Internet Filtering would block most criminal sites.

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. Staff are aware that their actions outside school may reflect on their position of responsibility in school and should therefore be given careful consideration.

Members of staff should never knowingly become "friends" with students on any social networking site or engage with pupils on internet chat.

Staff 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 at the discretion of the Headteacher.

Passwords - staff should keep passwords private. Passwords are confidential and individualised to each class teacher.

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.

Personal Use - staff are not permitted to use ICT equipment for personal use unless the Head teacher allows otherwise.

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. The school Photograph's Policy must be followed.

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 ARK ICT 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 e- safety. A list of CEOPs 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 the PSHE curriculum.

<u>During e-safety lessons, children will be taught</u>:

- 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 turn the computer monitor off 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, unless directed by the teacher
- that it is not advisable to upload pictures or videos of yourself either, as videos and pictures can easily be manipulated
- 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. Universities and future employers have been known to search social networking sites
- 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

- that in the same way that some Internet services can be used inappropriately, the same is true with mobile phones

- to never take inappropriate pictures of themselves and send to them to friends or upload onto social networking sites. Never forward inappropriate pictures that they have received from somebody else. In some circumstances 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.
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

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) AND COMPUTING POLICY

(to be read in conjunction with ICT and Computing schemes of work.)

Purposes

During the Foundation Stage and at KS1, ICT will be used to help deliver the core curriculum. Each department has at least two P.C computers and access to the school bank of laptop and tablet computers as well as appropriate software and apps to teach the core curriculum. The class teacher will often find ways to enhance ICT skills across the wider curriculum too.

Note: ICT is taught across the subjects, but there are also specific lessons to teach new skills: how to use PowerPoint, write an email, use Paint. Computing is taught in dedicated lessons.

In the Foundation Stage ICT includes:

- Using battery operated/remote control toys
- Using a computer and mouse
- Following logical steps to produce an end result
- Understanding that technology is an integral part of our world

The delivery of ICT at KS1 and 2 will include:

Knowledge, skills and understanding:

Finding things out

Developing ideas and making things happen

Exchanging and sharing information in a safe manner

Reviewing, modifying and evaluating work as it progresses

In 2014, the new computing scheme of work was introduced in line with the 2014 National Curriculum. Teachers take part in twilight training sessions to update skills particularly in relation to using SCRATCH and KODU in school. Our local Secondary Schools also use these programs meaning transition is effective. Class 5 pupils reinforce the teacher's input to younger children and less able year 5 and 6 pupils, by practicing the relevant programming skills with pupils from Classes 3 and 4. Pupils are familiar with programming language such as algorithm, search engine, hardware.

Breadth of Study

Pupils will be given opportunities to work with a range of information, explore with a variety of ICT tools and investigate and compare different uses of ICT inside and outside school.

Pupils will have experiences of using ICT for:

- communicating information, including the Internet and e-mail safely
- data handling
- measurement and control.

Social Networking Policy

Introduction

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites.

The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively, flexibly and safely.

However, it is also important to ensure that we safeguard our pupils and maintain the school`s outstanding reputation. Our use of social networking sites and applications has implications for our duty to safeguard children, young people and vulnerable adults.

Please also refer to the Safeguarding Policy / E-Safety Policy

The aim of this policy is to offer support to innovation whilst providing a framework of good practice. The policy and associated guidance is to protect staff and pupils and advise school staff on how to deal with potential inappropriate use of social networking sites.

Just Some Examples of a Social Networking Site and Applications

This policy applies to all uses of social networking sites and social networking applications.

Facebook is one of the widest used social networking sites. Facebook is targeted at older teenagers and adults. They have a no under 13 age registration policy and recommend parental guidance for 13 to 16 year olds.

Examples of social networking applications:-

- Blogs, for example Blogger
- Online discussion forums, such as netmums.com
- Collaborative spaces, such as Facebook
- Media sharing services, for example You Tube
- 'Micro- blogging' applications, for example Twitter.

All school representatives, staff and pupils should bear in mind that information they share through social networking applications, **even if they are on private spaces** are still subject to copyright, data protection and freedom of information legislation, the Safeguarding Vulnerable Groups Act 2006 and further legislation.

Use of Social Networking Sites in Work Time by School Staff

The use of social networking sites and applications in work time for **personal** use is not permitted, unless prior permission has been given by the Head Teacher or the Principal.

Use of Social Networking Sites by Pupils

Pupils will not be allowed to use any social networking sites or applications whilst at school - this includes the use of children's sites such as Club Penguin, Moshi Monsters and Habbo Hotel. The only time social networking sites may be used **is under direct supervision by a member of school staff as part of a lesson on safety.**

Social Networking as Part of School Service

Mrs Grayling, Curriculum Coordinator and Mrs Miles the Headteacher are the primary members of staff with responsibility for keeping the school Website updated and for posting information on Facebook.

Terms of Use

Social Networking Applications…

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns.
- Must not be used in an abusive or hateful manner.
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.

- Must not breach the school's policies.
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents.
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend to share information with'. The only exception to this rule is the school Facebook site where ex-pupils may be accepted as friends once they reach 13 years of age. This enables ex-pupils to keep in contact with their Primary School.
- Employees should not identify themselves as a representative of the school.
- References should not be made to any staff member, pupil, and parent or school activity/event unless permission has obtained and agreed with Mrs Grayling, Curriculum Coordinator.
- Staff should be aware that if their out-of-work activities cause potential embarrassment for the employer or detrimentally affect the employer's or schools reputation then the employer is entitled to take disciplinary action.

Guidance for Staff on Using Social Networking Sites

- **No member of staff should interact with any pupil in school on social networking sites.**
- **No member of staff should interact with any ex-pupil of the school on social networking sites who is under the age of 18, with the exception of the school Facebook site.**
- Class teachers should highlight the risks of cyber bullying and internet grooming in an age appropriate way to their pupils. Resources and advice for teachers and parents are available from Cyberentors.org.uk , CEOP, and Child Net International, the Safer Internet Centre. Children should be told to report any improper contact or cyber bullying to their teacher and parents.
- As part of assemblies, KS1 pupils are made aware of 'Stranger danger' in all its forms. Parents are encouraged to place home computers in a public area so that they have full knowledge of their child's internet activity. KS2 pupils are shown the videos from http://www.childnet.com/kia/primary/smartadventure/default.aspx which educate children in internet safety. There are regular opportunities to discuss pupil's safety outside school when using social networking sites, texting, emailing etc. Parents are also given internet safety advice in the form of leaflets from one of the above mentioned organisations. Internet safety is a subject that is discussed at Parents evenings.
- Year 6 children receive E-Safety training by the Stay Safe partnership.
- The School does not tolerate any form of bullying.
- It is illegal for an adult to network, giving their age and status as a child.

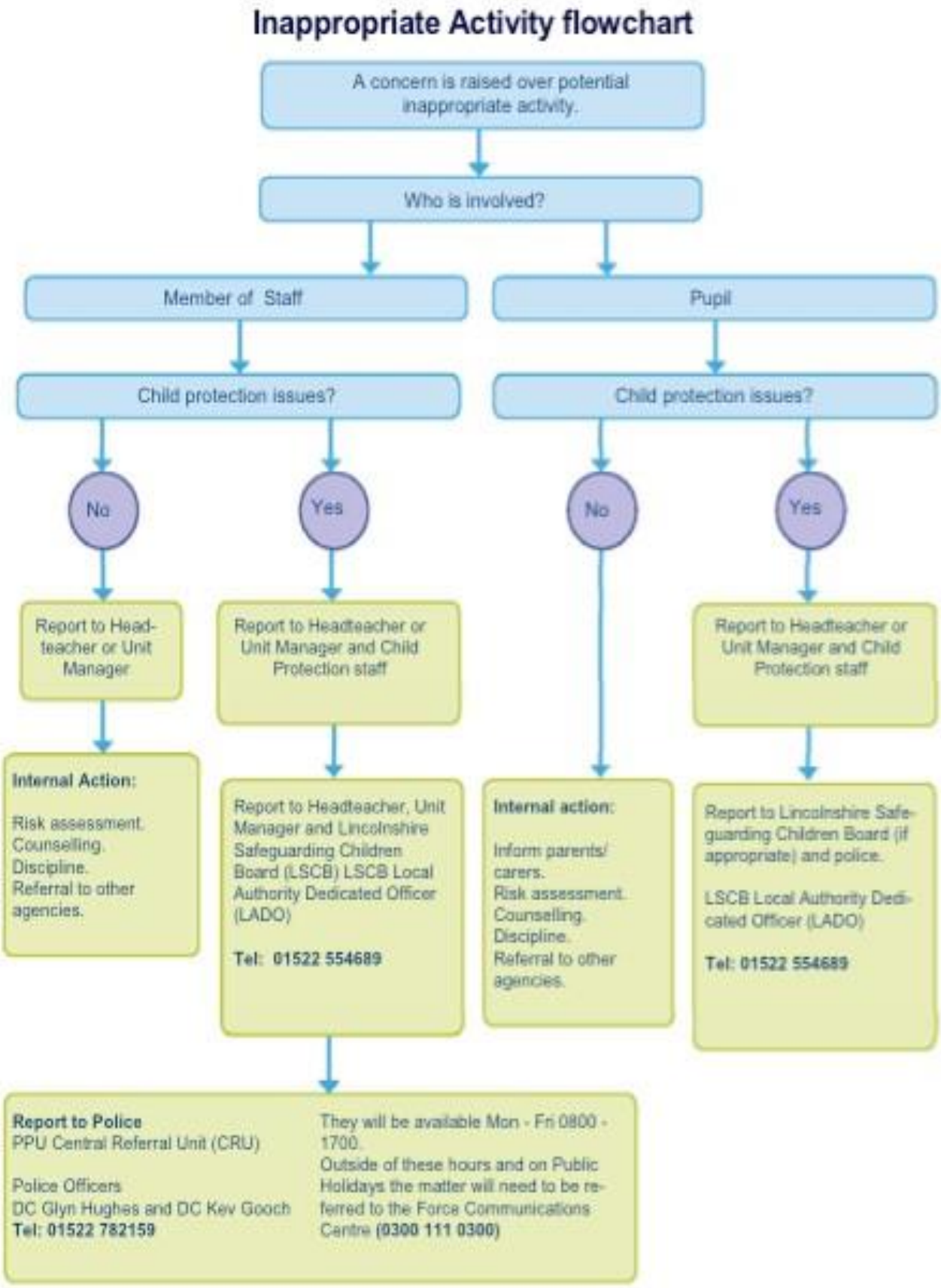
Guidance for Pupils on Using Social Networking Sites

- **No pupil may access social networking sites whilst at school, unless it is under the direct supervision of a member of school staff and in relation to a particular school topic or lesson. Pupils are not permitted to use 'Club Penguin' and such sites whilst at school.**
- **Computers accessible within school are all monitored by ARK ICT who monitor and govern internet use by the school. This limits access to websites suitable for children and informs the school of any searches pupils try to make that are inappropriate.**
- **Pupils are not permitted to bring mobile phones into school unless specific agreement has been requested by the parent as a one-off concession. In this case, the phone must be left in the basket in the office, as with all mobile phones.**

Written July 2012 W. Bell Curriculum Coordinator

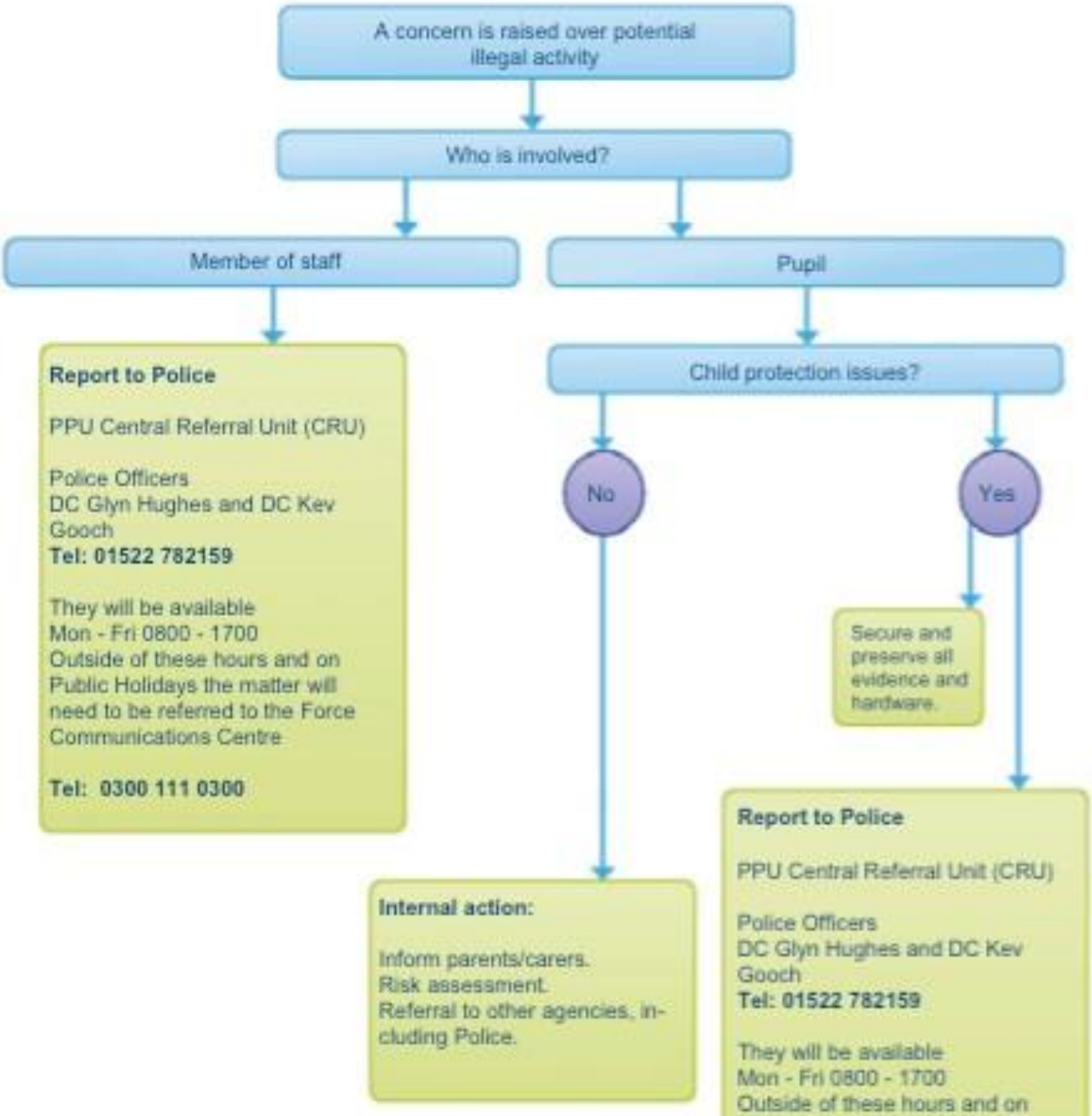
Reviewed June 2020 Next review June 2021.

Appendix 1


Inappropriate Activity flowchart
A concern is raised over potential inappropriate activity.
Who is involved?
Member of Staff
Pupil
Child protection issues?
Child protection issues?
No
Yes
No
Yes
Report to Head-teacher or Unit Manager
Report to Headteacher or Unit Manager and Child Protection staff
Report to Headteacher or Unit Manager and Child Protection staff
Internal Action:
Risk assessment.
Counselling.
Discipline.
Referral to other agencies.
Report to Headteacher, Unit Manager and Lincolnshire Safeguarding Children Board (LSCB) LSCB Local Authority Dedicated Officer (LADO)
Tel: 01522 554689
Internal action:
Inform parents/ carers.
Risk assessment.
Counselling.
Discipline.
Referral to other agencies.
Report to Lincolnshire Safe-guarding Children Board (if appropriate) and police.
LSCB Local Authority Dedi-cated 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 re-ferred to the Force Communications Centre (0300 111 0300)

Appendix 2

Illegal Activity flowchart



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 have 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 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.