JOHN SPENDLUFFE TECHNOLOGY COLLEGE

E SAFETY POLICY

JOHN SPENDLUFFE TECHNOLOGY COLLEGE

E SAFETY POLICY

STAFF POLICY

JOHN SPENDLUFFE TECHNOLOGY COLLEGE
E-SAFETY POLICY

Safeguarding Officer: R Thornalley (K Paice / S Curtis in his absence)
E-Safety Education Officer: H Elias
Staff able to offer technical guidance: Network Manager & ICT Technician

E-Safety Policy – Policy statement

The use of digital technology is now seen as an essential part of everyday life. 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 different people in different ways.

While digital technology can be used in positive ways, 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, 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 that some activities in the virtual world are criminal offences and can lead to 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 ensure 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. This policy has been adapted from their guidance for use at JSTC.

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 remain 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. Young people should be aware that “Taking, making, sharing and possessing indecent images and pseudo-photographs of people under 18 is illegal.” (Source: Home Office: “Indecent images of children: guidance for young people”)

E-Safety - 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; Tablets; Xboxs ; PlayStation; Nintendo Wii; mobile phones; Smart watches and PDAs, 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 of 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
- E-Safety is also about informing young people where to seek help and advice on e-Safety issues and reporting.

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, parents / carers 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.

The school’s e-Safety Policy operates in conjunction with other school policies including Behaviour, Child Protection, Acceptable Use and Anti-Bullying.

E-Safety - responsibilities for all staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss e-Safety issues with pupils. Further advice can be sought from Lincolnshire Safeguarding.

The trust between pupils and school staff is essential to education but very occasionally it can break down. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. Nationally, CEOP was set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders" and their work should be acknowledged and built upon by schools.

Within JSTC a member of staff who flouts security advice or uses ICT technology for inappropriate reasons risks dismissal.

All permanent, trainee, short-term and long-term supply staff should sign an Acceptable Use Policy on appointment; before any internet or computer access is granted. Staff thereby accept that the school can monitor network and 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 supervised. Procedures must define how inappropriate or illegal ICT use is reported to the Senior Leadership Team. 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, parents / carers 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 should provide establishment email accounts for all staff.

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). 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/anti-bullying 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 Policy (School 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 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 such as Facebook, Twitter, Instagram etc. should be blocked in all schools until such a time where students and staff have received sufficient education in the dangers and are able to safeguard themselves online. *It is advised that Social Networking is not allowed en masse; establishments should consider which sites would be appropriate based on factors such as age range, educational value, etc.*

If social networking is allowed, ensure that there is a strict policy with regards to security of personal details, rather than relying on the default settings. You should also ensure that any age restrictions are adhered to (many social networking sites have a minimum age of 13 years). Social networking use such as Facebook is authorised on our school computers, for staff only, before and after the allocated school open hours. This is to provide support for resources and support from educational groups such as BTEC and GCSE examination boards.

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. Support can be found with the Pastoral Team and ICT department.

Members of staff should never knowingly become “friends” with current students and their parents / carers on any social networking site or engage with them on Internet chat.

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 person. On no account should a member of staff allow a student to use a staff login. Passwords should include upper case, lower case, numeric and unique characters, consisting of an 8-character minimum.

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. All staff must only use an encrypted USB stick for the transfer of information between home and JSTC. Cloud network storage, other than Microsoft Teams, is not permitted for sensitive data.

File sharing - technology such as peer to peer (P2P) and bit torrents is not permitted on the JSTC’s Network. John Spendluffe student or staff information should not be stored on any cloud network, other than JSTC Microsoft Teams in regulation of the new Data Protection Act.

Personal Use - If personal use is permitted, the school should emphasise what is considered within the boundaries of acceptance.

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. Please consult a member of the Pastoral Team or ICT department for support on this issue.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the school. 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 the ICT Admin team 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 Policy (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.

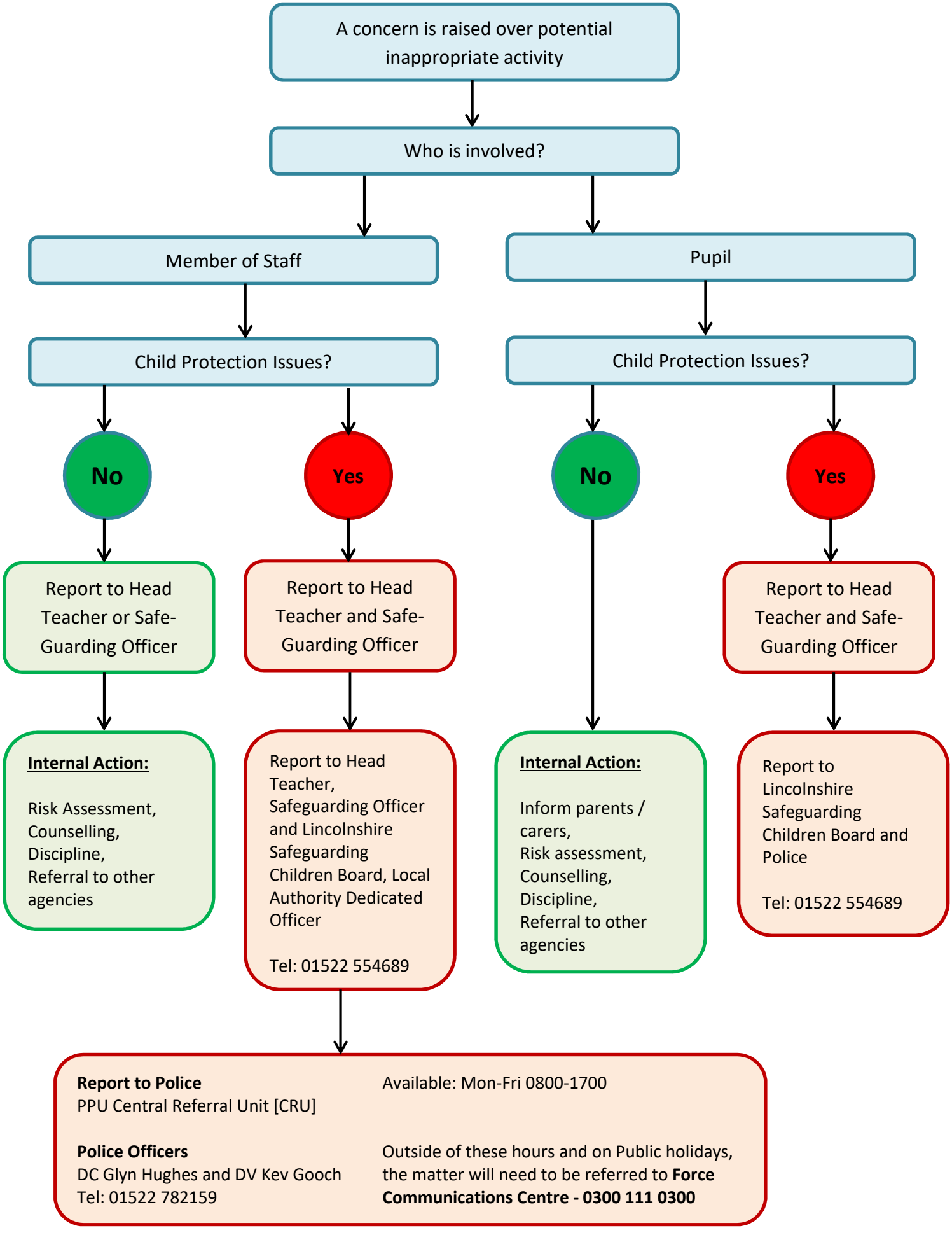
If you receive spam or junk email and texts, never believe the content, reply to them or use them.

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.

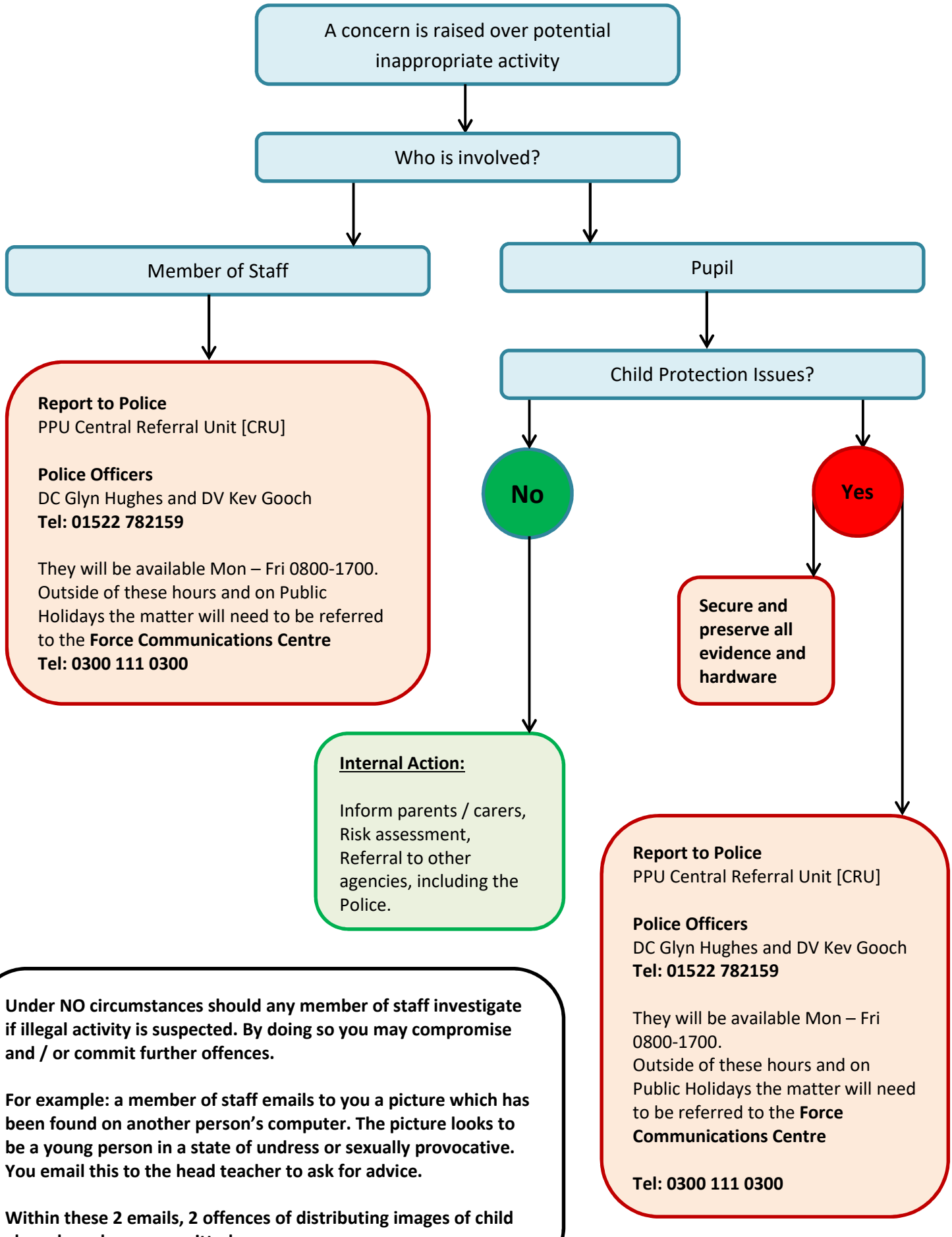
Understand that some people lie online and that therefore it's better to keep online mates online. Never meet up with any strangers without an adult that you trust.

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

Inappropriate Activity Flowchart



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 head teacher to ask for advice.

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

POLICY DOCUMENTS

The following policy document was presented to the Governing Body of John Spendluffe Technology College and approved and adopted by them on the date stated.

Policy: E-Safety Policy (Staff)

Signed as approved on behalf of the Governing Body

Mr S Curtis, Headteacher

Date: 28/03/2022

JOHN SPENDLUFFE TECHNOLOGY COLLEGE

E SAFETY POLICY

STUDENT POLICY

JOHN SPENDLUFFE TECHNOLOGY COLLEGE
E-SAFETY POLICY

Safeguarding Officer: R Thornalley (K Paice / S Curtis in his absence)
E-Safety Education Officer: H Elias
Staff able to offer technical guidance: Network Manager & ICT Technician

E-Safety Policy – Policy statement

The use of digital technology is now seen as an essential part of everyday life. 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 different people in different ways.

While digital technology can be used in positive ways, 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, 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 that some activities in the virtual world are criminal offences and can lead to 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 ensure 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. This policy has been adapted from their guidance for use at JSTC.

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 remain 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. Young people should be aware that “Taking, making, sharing and possessing indecent images and pseudo-photographs of people under 18 is illegal.” (Source: Home Office: “Indecent images of children: guidance for young people”)

E-Safety - 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; Tablets; Xboxes ; PlayStation; Nintendo Wii; mobile phones; Smart watches and PDAs, 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 of 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
- E-Safety is also about informing young people where to seek help and advice on e-Safety issues and reporting.

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 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 students 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, parents / carers and visitors that the use of school equipment for inappropriate reasons is “unauthorised” and ensure an Acceptable Use Policy is in place. 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.

The school’s e-Safety Policy operates in conjunction with other school policies including Behaviour, Child Protection, Acceptable Use and Anti-Bullying.

E-Safety Policy (students)

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 you are safe and that you are not exposed to illegal or inappropriate content. It is hoped that these restrictions do not interfere with your education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues.

Please note that Internet and email use are subject to monitoring

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 anything 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. Any actions breaching this, will result to an indefinite internet ban, at the Head Teacher's discretion.

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. Passwords should include upper case, lower case, numeric and unique characters, consisting of an 8-character minimum.

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. The user areas provided are given to you and are a privilege, not a right. Therefore, they should be used with respect and accordingly.

Social Networking - social networking (for example Facebook, YouTube, Twitter, SnapChat, Instagram, WhatsApp, etc.) is not allowed in school. For out-of-school use, note the following guidance - 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 school or anyone within the school as these can result in serious consequences. 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.

Students should never attempt to: contact, add, message or befriend an existing member of staff during their time at the school on any social media site or app. Any sharing or use of staff's personal information is strictly prohibited. Any student who conducts any behaviour of this nature will face serious consequences. The only form of electronic contact students should

have with a member of JSTC staff should be done via emails, Microsoft Teams or ClassCharts facility.

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. Students found in breach of this, will face serious consequences decided by the Head Teacher.

Copyright - you should never take information from the Internet and use it as your own. A lot of information is covered by Copyright Law, 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. Students found in breach of this, will face serious consequences decided by the Head Teacher.

Etiquette - **email accounts**. 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. Email activity is monitored by the school. Email use is monitored in school and inappropriate use will result in an email ban for a period of time. The period of time is set on the severity of the incident.

Mobile Phones, Tablets and Smartwatches - Modern mobile phones and smartwatches offer the same services as a computer, i.e. email access, Facebook, YouTube, Snapchat, Instagram, Twitter, 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. Mobile phones should be switched off and put away in your blazer / bag; unless your teacher has given you specific permission to use the device. Mobile phones are only permitted within the 'Food and Phone Zone' during break and lunch times.

Should you be caught using your mobile phone and / or tablet and / or smartwatch during a lesson, it will be confiscated and kept at the office until the end of the school day. Refusal to hand over your mobile device will result in a phone call home and phone to be kept in the office with permission of the Head Teacher.

Should you be involved in a social media issue with a fellow peer(s), your mobile device will be confiscated and kept in the safe at the office, for your own safety during the school day. This is to support you and your learning, reducing the risk of further issues or incidents.

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

You should not take any photos of other students or staff within lessons. These should not be shared with friends/family. Ask your teacher for guidance. Mobile phones should not be used during school / lesson time, staff will ask for you to turn the device off and put away in your school bag or blazer.

Useful websites:
CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent 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

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

E-Safety Policy (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. Only accept ‘friends’ or ‘followers’ from people you know. Remember, that if you receive messages or content that you do not wish to receive, report it to an adult and seek advice.

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

POLICY DOCUMENTS

The following policy document was presented to the Governing Body of John Spendluffe Technology College and approved and adopted by them on the date stated.

Policy: E Safety (Students)

Signed as approved on behalf of the Governing Body

Mr S Curtis, Headteacher

Date: 28/03/2022