Online-Safety

(including Social Networking and Acceptable Use)

Reviewed annually by the Headteacher – reported to Full Governing Body

Date of last Review	Signature
Autumn 2024	**Chair**

Online Safety

Introduction

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

Aims

- To ensure that the requirement to empower the whole school community with the knowledge to stay safe and as riskfree as possible is met.
- To ensure risks are identified, assessed and lessened (where possible) in order to reduce any foreseeable harm to the pupils or liability of the school. This policy sits in conjunction with our Anti-Bullying Policy.

- To be proactive in ensuring children's safety when using digital technologies in School so they can work safely at all times, and also to help children develop the skills to keep themselves safe when accessing digital technologies outside of School.

Our objectives are 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 behaviors both in and out of school.

Implementation

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 or as needed when significant developments in the area of e-safety are made.

E-safety is a vital part of our PSHE and Computing curriculums.

Managing Whole School Access to the Internet

To provide assistance in safeguarding we use active/monitored Internet content filtering.

Inappropriate content, categories and sites are blocked. If a teacher needs a site unblocking, they will need to speak to the IT technicians in good time and be able to explain how the site is safe and appropriate to be used. The IT technicians will refer to Senior Leaders for a decision whether to unblock a site.

Our IT security systems actively monitor all network traffic and anyone who uses it, blocking inappropriate sites and log-on attempts. The IT technicians are notified by email of any attempts to access restricted content. These attempts are followed up by the IT technicians and referred to the Head teacher.

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

Role of the governing body

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

- Review this policy regularly and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, and ensure that any Online Safety issues are dealt with appropriately;

- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will keep up to date with emerging risks and threats through technology use and receive regular updates from the Headteacher in regard to training, identified risks and any incidents.

Role of the Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for Online Safety within our school. The dayto-day management of this will be delegated to the named member of staff

The Headteacher will ensure that:

- Online Safety training throughout the school is planned, up to date and appropriate to the recipient;
- All Online Safety incidents are dealt with promptly and appropriately. Alford Primary School Online Safety Policy (including Social Networking and Acceptable Use)

Role of the Online Safety Leader

The Online Safety Leader will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themself with the latest research and available resources for school and home use;
- Review this policy regularly and bring any matters to the attention of the Headteacher;
- Advise the Headteacher and governing body on all Online Safety matters;
- Engage with parents and the school community on Online Safety matters at school and/or at home;
- Liaise with the local authority, IT technical support and other agencies as required;
- Retain responsibility for the Online Safety risk assessment;
- Ensure any technical Online Safety measures in school (e.g. Internet monitoring and filtering software) are fit for purpose through liaison with the local authority and/or IT technical support.

Role of the IT Technical support staff are responsible for ensuring that:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices;
- Operating system updates are regularly monitored, and devices updated as appropriate;
- Any Online Safety technical solutions such as Internet filtering are operating correctly;
- Filtering levels are applied appropriately according to the user (staff and pupils);
- Passwords are applied correctly to all users regardless of age;

Role of all other staff (in both a paid and unpaid capacity) Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher;
- Any Online Safety incident is reported to the Online Safety Leader or in his/her absence to the Headteacher.

Risk assessment of potential issues/dangers

The Online Safety Leader will ensure that the risk assessment is kept up-to-date in line with technological developments within the school (located at the end of this policy). The risk assessment will be shared with all staff members and the school’s IT technical support provider.

In the event of staff/pupils accidentally accessing online material that they deem to be inappropriate/offensive, it will be reported to the Online Safety Leader or, in their absence, to the Headteacher.

Protection against extremism/radicalisation

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the Internet as a means of either inciting violence against specific groups or providing information on carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Appropriate filtering is in place and will be reviewed whenever there is an incident of pupils accessing websites advocating extremism;
- The Online Safety Leader will record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school or its pupils;
- A referral will be made to the police whereby a pupil is deeply involved in the extremist narrative and there is evidence that their parents are involved in advocating extremist violence.

Child on child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online child on child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-onpeer abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Supporting pupils' mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Online safety training for staff As part of our Safeguarding training pathway, all staff undertake training in online safety. However, in addition to this, all staff receive annual face-to-face online safety training from an online safety advisor.

Social Networking

1 Staff and governors using social networking websites and/or apps

1.1 Staff are within their rights to use social networking websites and we are not, nor would not want to be, in a position to prevent staff from using them. However, we do ask that staff adhere to the following aspects of our policy:

1.2 Under no circumstances should pupils or ex-pupils under the age of 13 be befriended on a social networking website. If a child requests the befriending of a staff member, their parents should be informed.

1.3 In the event that a parent makes contact with a staff member through a social networking website, the staff member must use extreme caution and it is recommended that they provide their school email address as a point of contact for professional purposes. In the event of communicating with a parent or adult associated with a child who attends the school, no comments should be made about pupils, staff or parents.

1.4 Any statements or status remarks published on personal social media, in any capacity, should not contain any comments about the school, staff, parents or pupils – unless it is a direct share of a post from the school's own social media account.

1.5 All views expressed by staff members on social networking websites are their personal views and are in no way endorsed, nor supported, by the school. Staff should always assume that anything posted on social media would be attributed to them as a professional.

1.6 School employees and volunteers must not identify themselves as associated with the school in any way, unless expressly authorised by the Headteacher. Authority to use official school social media will be given to individual members of staff by the Headteacher.

2 Pupils using/accessing social networking websites and/or apps

2.1 Under no circumstances should a child access social networking websites in school unless it is for a purpose instigated by the child's teacher. The school network system prohibits pupils from accessing these websites but the bypassing of the system or accessing through a mobile phone is strictly prohibited.

2.2 If any reports are received of pupils making inappropriate comments about staff or other pupils, hard copies will be obtained and the child will be reported immediately (to the website host) to have their account terminated. The parents/carers of the child will also be notified, and this could result in further action. If the comment is about a member of staff a referral may be made to the county's legal services.

3 Parents using social networking websites and/or apps

3.1 If hard copies of inappropriate comments about members of staff, pupils within the school or school decisions are received, the matter may be referred to the county's legal services and subsequent action will follow.

3.2 School visits: parents must not, under any circumstances, access social networking accounts whilst assisting staff members. They must also ensure that they do not take photographs/videos on a personal device. If there is evidence to prove that this has happened, then the parent will no longer be used as a helper on subsequent visits. If this is considered a GDPR breach, it will be reported in accordance with our GDPR policy.

Acceptable Use

1 Aim

1.1 The aim of this section of the policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet and technological resources in a safe and effective manner.

2 General

2.1 Pupils will be supervised by an adult whilst using the Internet. Online Safety is taught as part of our Computing curriculum.

2.2 Filtering systems (two-level) are used by our Internet Service Provider in order to minimise the risk of exposure to inappropriate material.

2.3 Downloading of non-approved software is prohibited and blocked (approval to be sought by Online Safety Leader or Headteacher).

2.4 Virus protection is present and maintained on all relevant devices.

2.5 Portable storage media (USB memory sticks, discs, SD cards, etc) are not used. In exceptional circumstances, where permission is granted from the Head teacher, the IT technician will transfer needed files from them for staff.

2.6 Staff should keep personal passwords private. Under no circumstances should a personal password be shared with a staff member, pupil or IT technical support staff. If staff feel that a password has been compromised, they should report this to the Headteacher or Online Safety Leader immediately.

2.7 Passwords to whole-school resources can be shared so long as password access does not lead to any pupil information other than name and year group.

3 World Wide Web

3.1 School staff and pupils will not intentionally attempt to access material deemed inappropriate or material that is blocked by filtering systems.

3.2 Pupils will not copy information from other sources without acknowledging and citing the original source (copyright infringement). 3.3 Pupils will never disclose or publicise personal information.

4 Email/Microsoft Teams

4.1 School staff and pupils will only use approved email and Microsoft Teams accounts whist on site.

4.2 School staff and pupils will not send material that is illegal, obscene, defamatory or material that is intended to annoy or intimidate another person.

4.3 Pupils will never arrange a face-to-face meeting with someone they know only through the Internet.
4.4 All communication will be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

5 Personal devices

5.1 Pupils may only bring personal devices into school with permission from their teacher.

5.2 Pupils' personal devices will not be allowed to access Internet in school unless under exceptional circumstances (agreed by the Online Safety Leader or Headteacher).

6 Portable devices/tablets

6.1 School teachers will be provided with an Apple iPad for use within their class and at home for a range of purposes.

6.2 Apple iPads will be password locked with all data set to be erased following 10 unsuccessful password attempts.

6.3 Apple iPads will not be used by any friends or family members outside of school.

6.5 All apps (paid and unpaid) will be managed via the Apple Volume Purchase Program (VPP) by the Online Safety Leader or the School Business Manager.

6.6 The pupil bank of iPads will only be used under adult supervision.

7 Mobile phones/smart devices

7.1 School staff, volunteers, parents and contractors are allowed to bring in personal mobile phones/smart devices for their own use. Staff, volunteers, parents and contractors should use their personal mobile phones/smart devices with caution. The responsible use of personal mobile phones and devices is based on an agreement of trust that; During times when children are on the school premises, phones must be kept on silent and out of sight. Staff, volunteers, parents and contractors may only make and receive calls out of school hours or in an emergency in the staff room.

7.2 Users bringing personal mobile phones/smart devices into school must ensure that there is no inappropriate or illegal content on the device – even if this is not immediately accessible or visible.

7.3 Staff, volunteers, parents and contractors will not use mobile devices to take images or videos of pupils, staff or any area of the school environment.

7.4 If school staff have a family emergency or similar and are required to keep their personal mobile phone to hand, prior permission must be sought from the Headteacher.

7.5 Staff, volunteers, parents and contractors will not access the WiFi system using personal mobile devices, unless permission has been given by the Headteacher.

7.6 Children are permitted to have a mobile phone in school if they are in KS2 and walk to and from school unaccompanied. All mobile phones belonging to children must be switched off and left at the office during school hours or in a locked cabinet, supervised by the class teacher, provided in the classroom.

8 Examining electronic devices

8.1 The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

8.2 Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

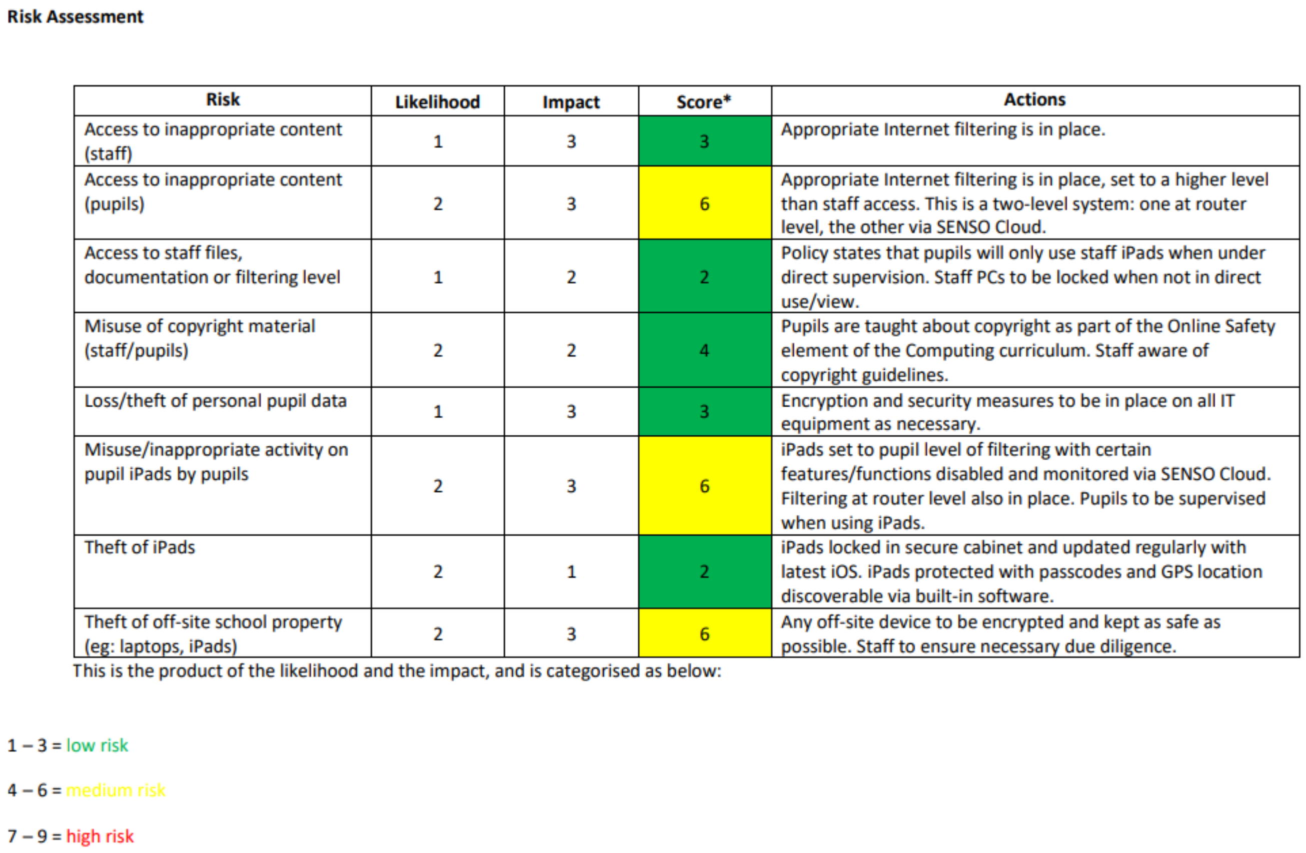
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from one of the school's DSLs
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation- informing parents as soon as is practicable and in the best-case scenario ensuring that parents are present

8.3 Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so. When deciding whether there is a ‘good reason’ to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

7 Risk Assessment * This is the product of the likelihood and the impact, and is categorised as below: 1 – 3 = low risk 4 – 6 = medium risk 7 – 9 = high risk Risk Likelihood Impact Score* Actions Access to inappropriate content (staff) 1 3 3 Appropriate Internet filtering is in place



Risk Assessment

Risk	Likelihood	Impact	Score*	Actions
Access to inappropriate content (staff)	1	3	3	Appropriate Internet filtering is in place.
Access to inappropriate content (pupils)	2	3	6	Appropriate Internet filtering is in place, set to a higher level than staff access. This is a two-level system: one at router level, the other via SENSO Cloud.
Access to staff files, documentation or filtering level	1	2	2	Policy states that pupils will only use staff iPads when under direct supervision. Staff PCs to be locked when not in direct use/view.
Misuse of copyright material (staff/pupils)	2	2	4	Pupils are taught about copyright as part of the Online Safety element of the Computing curriculum. Staff aware of copyright guidelines.
Loss/theft of personal pupil data	1	3	3	Encryption and security measures to be in place on all IT equipment as necessary.
Misuse/inappropriate activity on pupil iPads by pupils	2	3	6	iPads set to pupil level of filtering with certain features/functions disabled and monitored via SENSO Cloud. Filtering at router level also in place. Pupils to be supervised when using iPads.
Theft of iPads	2	1	2	iPads locked in secure cabinet and updated regularly with latest iOS. iPads protected with passcodes and GPS location discoverable via built-in software.
Theft of off-site school property (eg: laptops, iPads)	2	3	6	Any off-site device to be encrypted and kept as safe as possible. Staff to ensure necessary due diligence.

This is the product of the likelihood and the impact, and is categorised as below:

1 – 3 = low risk

4 – 6 = medium risk

7 – 9 = high risk

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 anti-bullying week each year. We foster an ethos of openness so children can talk about their IT usage and aren’t afraid to talks about their concerns and experiences.

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

- to never post private information that you wouldn't want to be seen in a public arena
- that Internet and email use is 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 the g-drive (user area) is provided to access shared files. It is not to be used to save children's work or other files that they have brought in from home
- that social networking (for example Bebo, Facebook, WhatsApp, Flickr) is not allowed in school and that there are age limits on such sites, e.g. you should be over 13 years old to have a profile on Facebook
- that they should never upload pictures or videos of others without their permission
- that it is not advisable to upload pictures or videos of yourself either, as videos and pictures can easily be manipulated and used against them
- 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

- when using school email, to always be polite and don’t use inappropriate language (e.g. swearing, discriminatory language); to consider what they 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 they write may be read incorrectly

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

- that mobile phones should not be brought into school but if they are needed (e.g. for children on transport) they are handed in to the Office or your class teacher for safe keeping, at the start of every day

- 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. 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

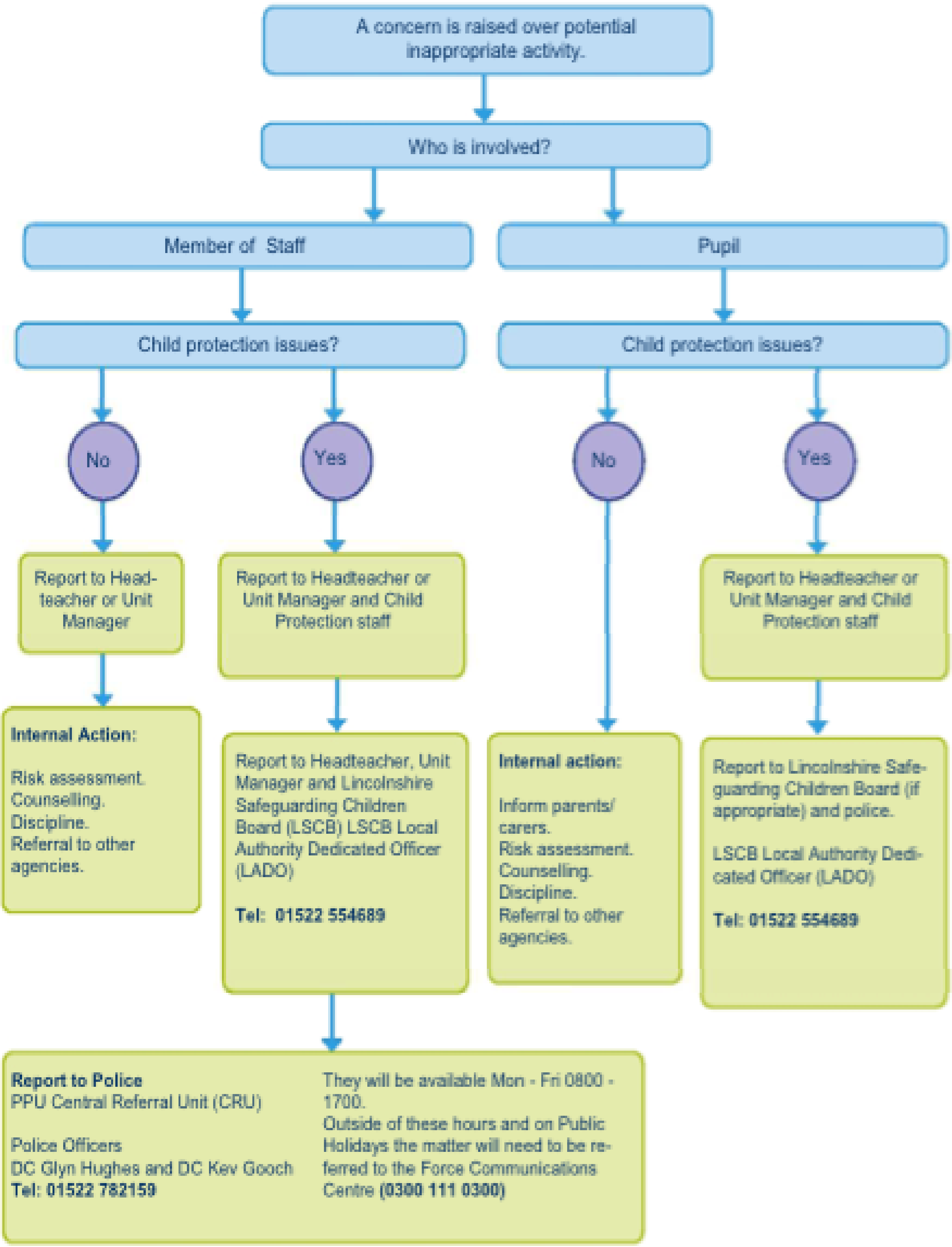
ICO
The Information Commissioner's Office in the United Kingdom, is a non-departmental public body which reports directly to Parliament and is sponsored by the Department for Digital, Culture, Media and Sport. http://ico.org.uk

Action Fraud - Action**Fraud** is the UK's national **fraud** and **cyber** crime reporting centre
https://www.actionfraud.police.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

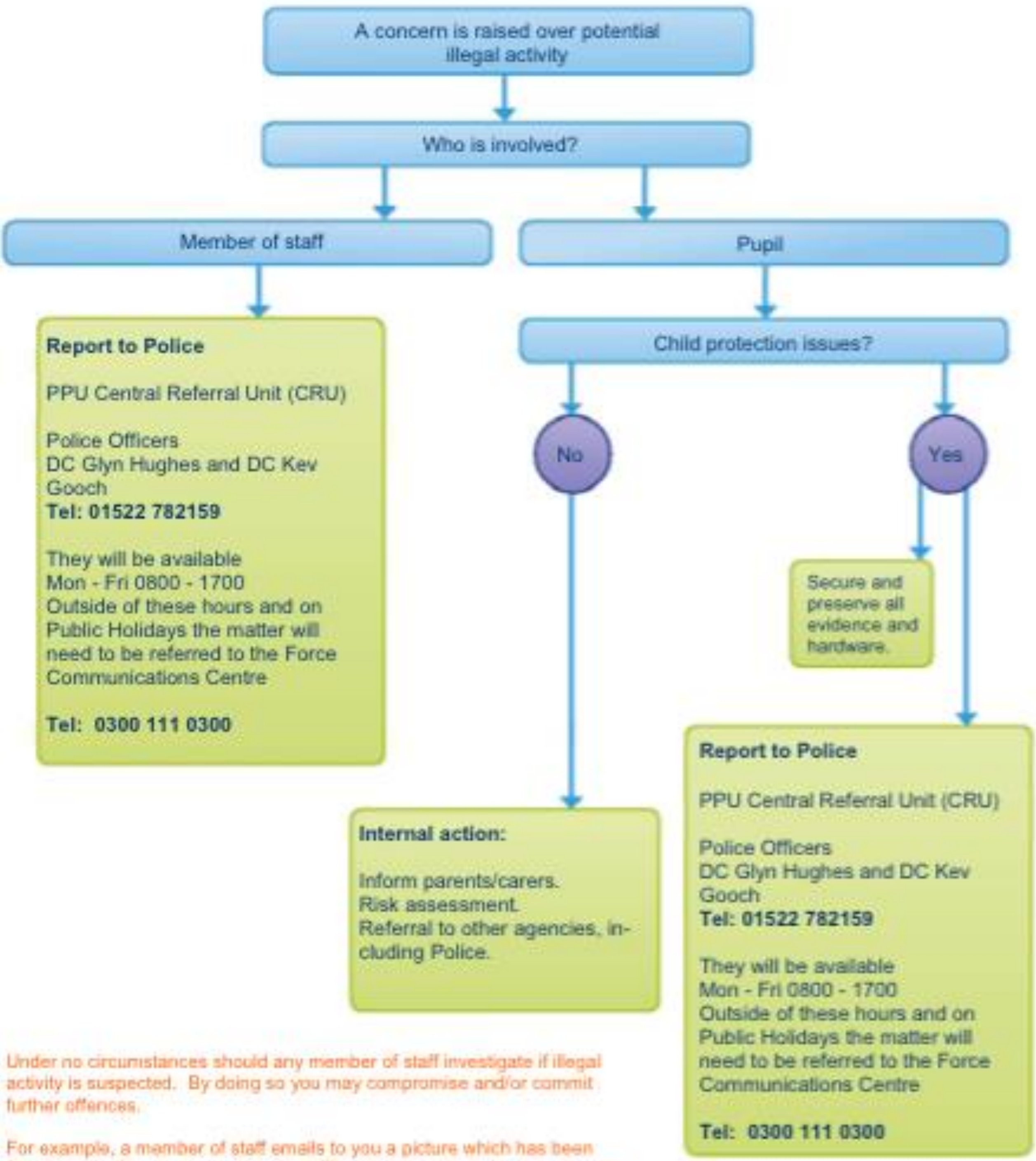
Report to Police
PPU Central Referral Unit (CRU)

Police Officers
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)**

Appendix 2

Illegal Activity flowchart



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

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 have been committed.

Appendix 3

Dos and Don’ts (Unacceptable Use)

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.

Removable media – We no longer allow the use of memory sticks or any writable removable media as a regular method of storage. This is policy and software controlled as well as monitored. If there is an exceptional reason for use, this can only be done with the express permission of the Head Teacher and under supervision.

Monitoring - Staff should note that computer use, Internet and email usage are subject to monitoring.

Breaches of Policy – Disciplinary procedures apply.

Data Protection - Please refer to our GDPR Procedure for Information on data breaches.