

Langtoft Primary School

Online Safety Policy

Article 16 (Privacy) You have the right to privacy.

Article 17 (Information) You have the right to get information that is important to your well-being, from...computers and other sources. Adults should make sure that the information you are getting is not harmful, and help you find and understand the information you need.

Article 36 (Protection) You have the right to protection from any kind of exploitation (being taken advantage of)

1. Introduction

- 1.1 Langtoft Primary School understands the responsibility it has to educate pupils about online safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.
- 1.2 Langtoft Primary School has a whole school approach to the safe use of IT and creating a safe learning environment includes three main elements:
 - a range of technological tools
 - policies and procedures with clear roles and responsibilities
 - an online safety programme for pupils, staff and parents/carers.
- 1.3 The Internet can potentially give children access to material of an unsuitable nature and could also lead to children receiving unsuitable material. It is the school's policy to make every reasonable effort to protect pupils from such material but also to make them aware of the potential dangers at an appropriate level for their age.

2. Policy Governance

2.1 Development, Monitoring and Review of the Policy

The *Online Safety Policy* has been developed by:

Position	Name(s)
Headteacher	J McCullough
ICT Technical staff	ARK IT Solutions Ltd
Online Safety Governor	A Upward

2.2. Schedule for Review

- The *Online Safety Policy* was approved by the *Wellbeing and Provision Committee* on **23 April 2018**.
- Implementation of *Online Safety Policy* will be monitored by the headteacher and overseen by the Lead of the *Wellbeing and Provision Committee*

- The Governing Body will receive a report on the implementation of the *Online Safety Policy* generated by the *Wellbeing and Provision Committee* annually
- The *Online Safety Policy* will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be April 2019
- Serious online safety incidents must be reported to the Designated Safeguarding Leads, Chair of Governors, Local Authority Designated Officer (LADO) and Lincolnshire Safeguarding Children Board

3. Scope of the Policy

- 3.1 The policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors) who have access to, and are users of, school IT systems and mobile technologies, both in and out of school.

4. Roles and Responsibilities

- 4.1 Online safety is recognised as an essential aspect of strategic leadership in Langtoft Primary School. At least one member of staff has received Child Exploitation and Online Protection (CEOP) training.
- 4.2 It helps staff to think about the issues that young people face online and the challenge that faces the school to protect and educate pupils. It helps to review the provision in place and signposts to further help, support and advice.

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

- 4.4 **Governors** are responsible for the approval of the *Online Safety Policy* and for reviewing the effectiveness of the policy.
- 4.5 **Headteacher and leaders** are responsible for:
- keeping abreast of current issues and guidance through organisations such as Lincolnshire County Council, [CEOP](#), [Keeping Children Safe Online \(KCSO\)](#) and [ChildNet](#)
 - ensuring all teachers understand their responsibilities for promoting and supporting safe behaviours in their classrooms and following school online safety procedures
 - ensuring the online safety of members of the school community
 - being aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff ([See Flowcharts 2a/ 2b, Appendix 2](#))
 - taking day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school *Online Safety Policy* documents
 - coordinating training and signposting advice for staff by following a planned programme of formal online safety training
 - all new staff receiving online safety training as part of their in-house induction programme, ensuring that they fully understand the school *Online Safety Policy* and [Acceptable Use Agreement \(Appendix 1\)](#)
 - taking every opportunity to help parents/carers understand the issues surrounding online safety through parents' evenings, newsletters and the website

- receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments
- reporting annually to the governing body

4.6 **Technical staff** (ARK IT Solutions) are responsible for ensuring that:

- the school's IT infrastructure is secure and is not open to misuse or malicious attack
- they act as the IT Manager under guidance from the headteacher
- users may only access the school's networks through a properly enforced password protection policy
- any external access to the schools network or data is carried out via a secure virtual private network or other such secure technology

4.7 **Teaching and Support Staff** are responsible for ensuring that they:

- have an up to date awareness of online safety matters and of the current school *Online Safety Policy* and practices
- have read, understood and signed the school [Acceptable Use Agreement \(Appendix 1\)](#)
- report any suspected misuse or problem to the headteacher or deputy headteacher for investigation
- deliver a planned online safety programme as part of IT lessons and Personal, Social and Health Education (PSHE) lessons
- present key online safety messages as part of a planned programme of assemblies
- teach pupils to be critically aware of the materials/content they access online and be guided to validate the accuracy of information

4.8 **Designated Safeguarding Leads (DSL)** are trained in online safety in accordance with the Five Year Plan (see *Child Protection and Safeguarding Policy*) and aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

The DSLs will carry out an annual audit of the online safety training needs of all staff. They will also update annually the Safeguarding Audit (Section 6: online safety)

4.9 **Wellbeing and Provision Committee**

Members of *Wellbeing and Provision Committee* and the Online Safety Governor will assist the headteacher with the production, review and monitoring of the school's *Online Safety Policy*.

4.10 **Pupils**

- are responsible for using the school IT systems and mobile technologies in accordance with the *Acceptable Use Agreement (Appendix 1)*
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and should know how to do so

4.11 **Parents/Carers** are responsible for:

- completing an annual permission form (usually in September) that gives the school information on which activities their children may take part in.

- informing the school in writing of any changes to their consent before the next annual review (usually in September)
- reporting concerns to the headteacher (or to the Chair of Governors if the concern is about the headteacher)















5. Communication devices and methods

5.1	Staff and other adults				Pupils			
Communication method/device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed ONLY with permission from Headteacher	Not allowed
The following tables show the school's policy on the use of communication devices and methods. Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the subsequent tables.								
User Actions								
Mobile phones may be brought to school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on own mobile phones								
Taking photos on designated devices								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of chat rooms / facilities								
Use of instant messaging								
Use of social networking sites								
Use of blogs								

This table indicates when some of the methods/ devices in 5.1 may be allowed:

5.2	Circumstances when these may be allowed	
Communication method/device	Staff and other adults	Pupils
Mobile phones may be brought to school		When a written request by a parent/carer has been authorised by the headteacher
Use of mobile phones in social time	During break and lunchtime in staff room or offices	Never
Taking photos on own designated devices	Employed staff – on named iPad for use in school ONLY. With class camera. Other adults – when instructed by and supervised by employed staff	Never
Use of instant messaging	During break and lunchtime in staff room or offices	Never

5.3. Unsuitable/inappropriate activities

5.3 The school believes that the activities referred to in the table would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems.	Acceptable	Acceptable at certain times	Acceptable for nominated persons	Unacceptable	Unacceptable and illegal
User Actions					
View, produce or circulate child sexual abuse images					
Promotion or conduct of illegal acts, for example, fraudulent actions					
View, produce or circulate adult material that potentially breaches the <i>Obscene Publications Act</i> in the UK					
Produce or circulate criminally racist material in UK					
View, produce or circulate pornography					
Promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					
Promotion of racial or religious hatred					
Threatening behaviour, including promotion of physical violence or mental harm					
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute					

Using school systems to run a private business					
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LA and/or the school					
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					
Revealing or publicising confidential or proprietary information (for example: financial/personal information, databases, computer/network access codes and passwords)					
Creating or propagating computer viruses or other harmful files					
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet					
Online gaming (educational)					
Online gaming (non-educational)					
Online gambling					
Online shopping/commerce					
File sharing					
Use of social networking sites					
Use of video broadcasting for example: YouTube					
Accessing the internet for personal or social use (for example, online shopping)					
Using external data storage devices (for example, USB) that have not been encrypted, password protected and checked for viruses					

6. Good practice guidelines




6.1 Email

DO	Best Practice Staff and pupils should only use their school email account to communicate with each other.
CHECK	Safe Practice Send email outside of '@langtoft.lincs.sch.uk' only when connected to Langtoft Primary School server.
DO NOT	Poor Practice Do not use school email (personal or general) account to communicate with pupils and their families without copying in the headteacher. Do not use school email address when making online bookings or purchases that are not school-related and that do not have the headteacher's authorisation.

6.2 Images, photographs and videos

The use of digital/video images plays an important part in learning activities. Pupils and staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.




Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. The school will request parents / carers permission annually before taking images of members of the school.

 DO	Best Practice Only use school equipment for taking pictures and videos. Ensure parental permission is in place.
 CHECK	Safe Practice Check <i>Online Safety Policy</i> for any instances where using personal devices may be allowed. Always make sure have Headteacher's (or in the case of the headteacher, the Chair of Governor's) knowledge or permission. Make arrangements for pictures to be downloaded to the school network immediately after the event. Delete images from the camera/device after downloading.
 DO NOT	Poor Practice DO NOT download images from organisation equipment to own equipment. DO NOT use your equipment without Headteacher's/Chair of Governor's knowledge or permission – and in accordance with policy. DO NOT retain, copy or distribute images for personal use.




6.3 The Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people.




- Pupils will have supervised access to internet resources through the school's technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise any further research.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the headteacher or deputy and an email sent to ARK so that they can block the site.
- It is the responsibility of the school to ensure that anti-virus protection and anti-malware protection is installed and kept up-to-date on all school machines. Any changes to filtering must be authorised by a member of the senior leadership team.

	<p>Best Practice Understand how to search safely online and how to report inappropriate content.</p>
	<p>Safe Practice Staff and pupils should be aware that monitoring software will log online activity. Be aware that keystroke monitoring software does just that. This means that if shopping online then passwords, credit card numbers and security codes will all be visible to the monitoring technicians.</p>
	<p>Poor Practice Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings. Breach of the <i>Online Safety Policy</i> and <i>Acceptable Use Agreement</i> may result in confiscation of equipment, closing of accounts and instigation of sanctions.</p>




6.4 Mobile phones

	<p>Best Practice If staff do need to use a mobile phone while on school business (visits etcetera), make sure it is the phone that is registered against their name on Staff Contact list. Staff should make sure they know about inbuilt software/ facilities and switch off if appropriate.</p>
	<p>Safe Practice Check <i>Online Safety Policy</i> for any instances where using personal phones may not be allowed. Staff make sure they know how to employ safety measures like concealing their number by placing 141 in front of the required number.</p>
	<p>Poor Practice Staff must not use own phone without Headteacher's/Chair of Governor's knowledge or permission to contact a parent/carer. Contact details of parents/carers must be deleted after use.</p>

6.5 Social networking (for example: Facebook/Twitter)

	<p>Best Practice If staff have a personal account, regularly check all settings and make sure security settings are not open access. Ask family and friends to not post tagged images of staff on their open access profiles.</p>
	<p>Safe Practice Don't accept people they don't know as friends. Be aware that belonging to a 'group' can allow access to profile.</p>
	<p>Poor Practice Don't have an open access profile that includes inappropriate personal information and images, photos or videos.</p> <p>Staff:</p> <ul style="list-style-type: none"> • don't accept pupils or their parents/carers as friends on personal profile • don't accept ex-pupils users as friends • don't write inappropriate posts about colleagues, pupils or their parents

6.6 Webcams

 DO	<p>Best Practice Make sure know about inbuilt software/ facilities and switch off when not in use.</p>
 CHECK	<p>Safe Practice Check the <i>Online Safety Policy</i> for any instances where using personal devices may be allowed. Always make sure have Headteacher/Chair of Governors knowledge or permission. Make arrangements for pictures to be downloaded to the school network immediately after the event. Delete images from the camera/device after downloading.</p>
 DO NOT	<p>Poor Practice Don't download images from organisation equipment to own equipment. Don't use own equipment without Headteacher/Chair of Governors knowledge or permission – and in accordance with <i>Online Safety Policy</i>. Don't retain, copy or distribute images for personal use.</p>
















7. Data Protection










7.1 The school and all staff members comply with the General Data Protection Regulation (GDPR 2016). Personal data will be recorded, processed, transferred and made available according to the act. Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have secure passwords which are not shared with anyone. All users read and sign an *Acceptable Use Agreement* to demonstrate that they have understood the school's *Online Safety Policy*.

8. Incident Management

8.1 Due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device.

8.2 The school cannot accept liability for material accessed or any consequences of this. Concerns should be shared with the headteacher. Incidents should be logged and the flowchart for managing an online safety incident followed.

Incidents (pupils):	Refer to Class Teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff	Inform parents/carers	Removal of access rights	Warning	Further sanction: e.g., exclusion
Deliberately accessing or trying to access material that could be considered illegal								
Unauthorised use of non-educational sites during lessons								
Unauthorised use of mobile phone/digital camera / other handheld device								

Unauthorised use of social networking/ instant messaging/personal email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Unauthorised downloading or uploading of files	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Allowing others to access school network by sharing username and passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Attempting to access or accessing the school network, using another pupil's account	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Attempting to access or accessing the school network, using the account of a member of staff	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Corrupting or destroying the data of other users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Sending an email, text or instant message that is regarded as offensive or of a bullying nature	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Continued infringements of the above, following previous warnings or sanctions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Using proxy sites or other means to subvert the school's filtering system	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Accidentally accessing offensive or pornographic material and failing to report the incident	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Deliberately accessing or trying to access offensive or pornography	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Receipt or transmission of material that infringes the copyright of another person or infringes the <i>General Data Protection Regulation (GDPR)</i>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Incidents (staff and volunteers):	Refer to Headteacher	Refer to police	Refer to technical support staff	Removal of network/internet access rights	warning	Disciplinary/Ban
Deliberately accessing or trying to access material that could be considered illegal. (See list in earlier section on unsuitable/inappropriate activities).	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unauthorised downloading or uploading of files	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Careless use of personal data for example; holding or transferring data in an insecure manner	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Deliberate actions to breach data protection or network security rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Using personal email, social networking, instant messaging or text messaging to carrying out digital communications with pupils	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Actions which could compromise the staff member's professional standing	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Using proxy sites or other means to subvert the school's filtering system	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Accidentally accessing offensive or pornographic material and failing to report the incident	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			
Deliberately accessing or trying to access offensive or pornographic material	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Breaching copyright or licensing regulations	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Continued infringements of the above, following previous warnings or sanctions	<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>

Appendix 1 Acceptable Use Agreement

1a Pupils in Foundation Stage and Key Stage 1

These rules help us to stay
safe on the Internet

Think then Click



We only use the Internet when an adult is with us.



We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.



We always ask if we get lost on the Internet.



We can send and open emails together.



We can write polite and friendly emails to people that we know.

Think then Click



We ask permission before using the Internet.

We only use websites our teacher has chosen.



We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.



We send e-mails that are polite and friendly.

We never give out a home address or phone number.



We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.



We never use internet chat rooms.

We tell the teacher if we see anything we are unhappy with.



1c Staff (includes Volunteers and Governors)

Acceptable Use Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed online safety in my work with children.

For my professional and personal safety:

- I understand that the school will monitor my use of IT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school IT systems) out of school
- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down in the school's Online Safety Policy
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the headteacher, deputy headteacher or to ARK IT Solutions

I will be professional in my communications and actions when using school IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only use chat and social networking sites in school in accordance with the school's policies
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any online activity that may compromise my professional responsibilities

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the *Online Safety Policy* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school IT systems
- I will not open any attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

- I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will not try (unless I have permission) to make large downloads or uploads that might take up capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies and I am specifically authorised/requested to do so
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's *Privacy Notice*. Where personal data is transferred outside the secure school network, it must be encrypted
- I understand that any data about pupils, their families and staff to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened

I understand that I am responsible for my actions in and out of school:

- I understand that this *Acceptable Use Agreement* applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school
- I understand that if I fail to comply with this *Acceptable Use Agreement*, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Boards of Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

I have read and understood the *School's Online Safety Policy*

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

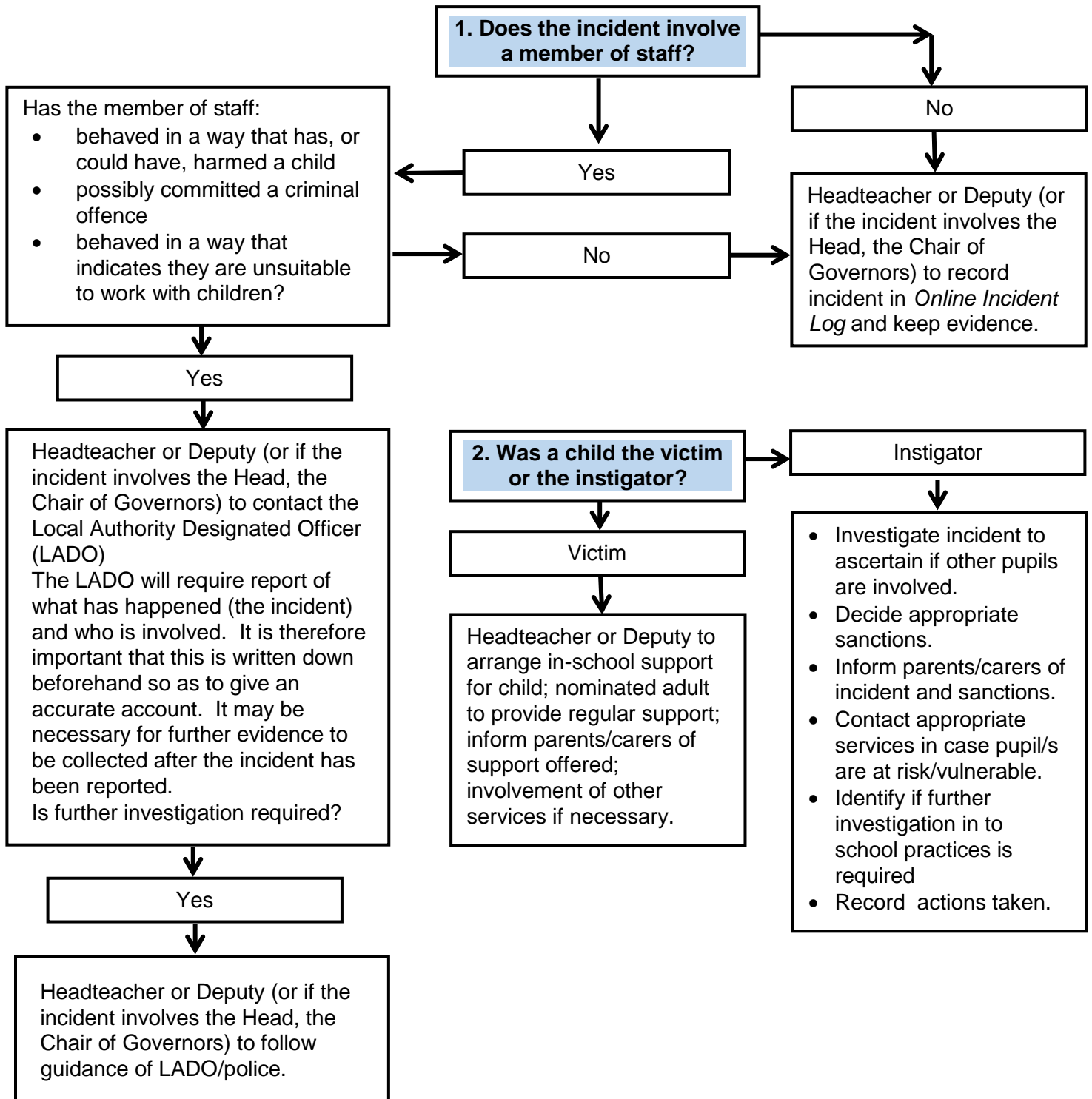
Name:	
Position:	
Signed:	
Date:	

Appendix 2 Flowcharts for managing online incidents

Flowchart 2a for managing an online incident involving non-illegal activity

Incidents not involving any illegal activity, such as:

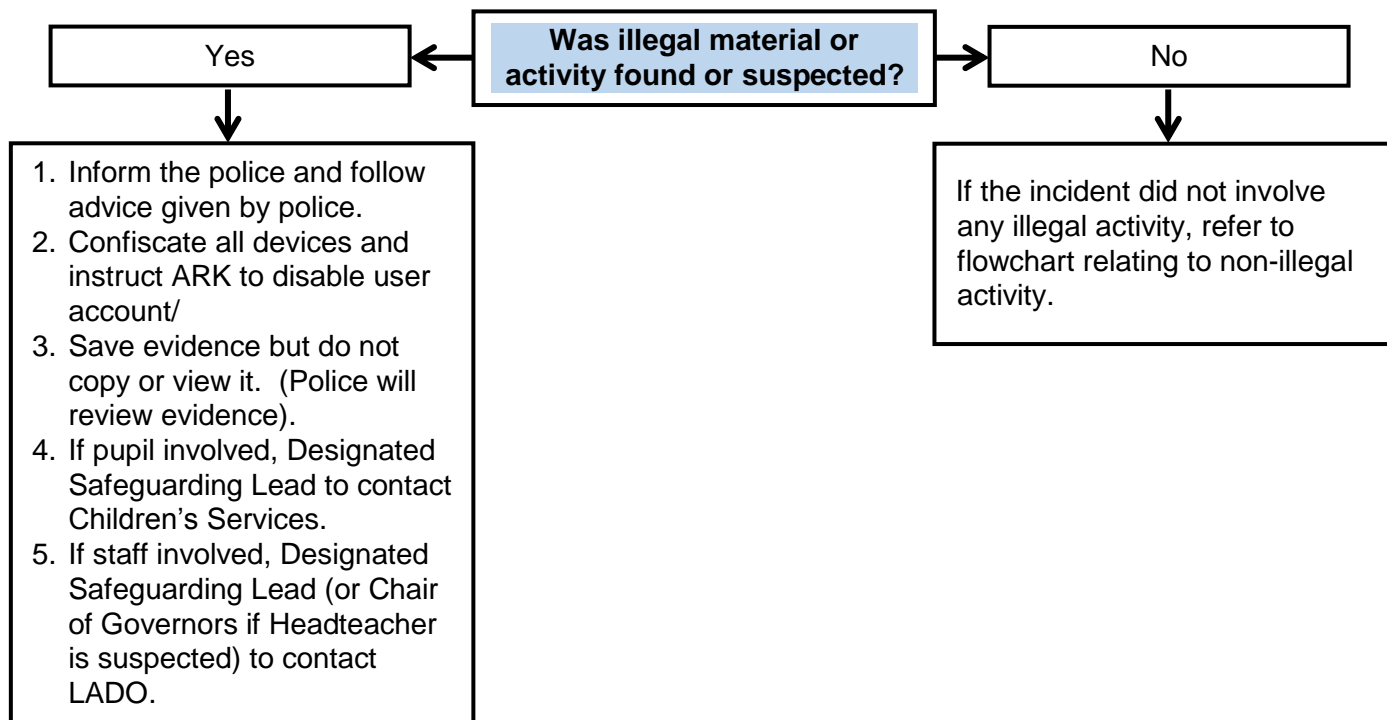
- using another person's user name and password
- accessing websites which are against school policy
- using a mobile phone to take video during a lesson
- using the technology to upset or bully (in extreme cases this could be illegal)



Flowchart 2b for managing an online incident involving illegal activity

Illegal means something against the law such as:

- downloading indecent images of children
- passing onto others images or video containing child pornography
- inciting racial or religious hatred
- promoting illegal acts



Appendix 3

LANGTOFT PRIMARY SCHOOL ONLINE INCIDENT LOG

This log will be completed by the head teacher or deputy following each incident. All incidents will be reported to governors in the Headteacher's report to Governors.

Date and time	Name of pupil or staff member	Room and computer/device number	Details of incident (including evidence)
Action taken and reason:			
Action taken and reason:			
Action taken and reason:			

Appendix 4a Advice for Children on Cyber-bullying

Three steps to stay out of harm's way

- 1) Respect other people. Online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.
- 2) If someone insults you online or by phone, stay calm and ignore them.
- 3) Think how you would feel if you were bullied. You're responsible for your own behaviour. Make sure you don't distress other people or cause them to be bullied by someone else.

Online bullying

Remember, bullying is never your fault. It can be stopped and it can usually be traced.

- ✓ Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.
- ✓ Try to keep calm. If you are frightened, try to show it as little as possible.
- ✓ Don't get angry. It will only make the person bullying you more likely to continue.
- ✓ Don't give out your personal details online. If you're in a chatroom, watch what you say about where you live, the school you go to, your email address and so on. All of these things can help someone who wants to harm you build up a picture about you.
- ✓ Keep and save any bullying emails, text messages or images. Then you can show them to a parent/carer or teacher as evidence.
- ✓ If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

Text/video messaging

You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number.

- ✓ If the bullying persists, you can change your phone number. Ask your parent/carer to talk to your mobile phone provider.
- ✓ Don't reply to abusive or worrying text or video messages. Your mobile phone provider will have a number for you to ring or text to report phone bullying. Visit their website for details.
- ✓ Don't delete messages from cyberbullies. You don't have to read them, but you should keep them as evidence.

Text harassment is a crime. If the calls are simply annoying, tell a teacher or parent/carer. If they are threatening or malicious and they persist, report them to your parent/carer and then the police, taking with you all the messages you've received.

Phone calls

If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn off your phone. Once the caller realises they can't rattle you, callers usually get bored and stop bothering you.

- ✓ Don't give out personal details such as your phone number to just anyone.
- ✓ Never leave your phone lying around.
- ✓ When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not.
- ✓ You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.
- ✓ Do not leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again.
- ✓ If the problem continues, think about changing your phone number. If you receive calls that scare or trouble you tell your parents, make a note of the times and dates and with your parents report them to the police. If your mobile can record calls, take the recording too. Almost all calls nowadays can be traced.

Emails

- ✓ Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- ✓ Keep the emails as evidence. Tell an adult about them.
- ✓ Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com
- ✓ Never reply to someone you don't know, even if there's an option to 'unsubscribe'. Replying simply confirms your email address as a real one.

Web bullying

If the bullying is on a website (for example, Facebook, Bebo) tell a teacher or parent/carer, just as you would if the bullying was face-to-face, even if you don't know the bully's identity. Serious bullying should be reported to the police, for example, threats of a physical or sexual nature. Your parent/carer or teacher will help you do this.

Chat rooms and instant messaging

- ✓ Never give out your name, address, phone number, school name or password online.
- ✓ It's a good idea to use a nickname. And don't give out photos of yourself.
- ✓ Don't accept emails or open files from people you don't know.
- ✓ Remember it might not just be people your own age in a chatroom.

- ✓ Stick to public areas in chat rooms and get out if you feel uncomfortable.
- ✓ Tell your parent/carer if you feel uncomfortable or worried about anything that happens in a chat room. (This includes whatsapp type chat groups).
- ✓ Think carefully about what you write; don't leave yourself open to bullying.
- ✓ Don't ever give out passwords to your mobile or email account.

Appendix 4b Advice for Parents and Children on Cyber-bullying

What to do if a child has come to you and needs help

- 1) Communication with your child is essential. Talk to them and reassure them that they can always come to you if something upsets or worries them online.
- 2) Save the evidence wherever possible. You may be able to report what has happened to the online service being used when the incident occurred. Evidence may include screen shots taken on a laptop or mobile device, emails, texts or online conversation histories. If you do need to make a report, evidence gathered will make it easier to show exactly what has taken place.
- 3) Knowing who to report to is a really useful step to resolve many issues, so do familiarise yourself with the services available below. Depending on what has happened, it might be necessary to let your child's school know too.

Where to report online safety concerns or risks

Grooming or other illegal behaviour

If you want to report someone who is behaving suspiciously online towards a child, you should contact 999 if it is an emergency situation, or otherwise make a report to [CEOP, the Child Exploitation Online Protection Centre](#).

Criminal content online

If you see any criminal content online, you should report this to the [Internet Watch Foundation \(IWF\)](#). Criminal content in the UK includes child sexual abuse images, criminally obscene adult content, as well as non-photographic child sexual abuse images.

Online content which incites hatred on the grounds of race, religion, disability and sexual orientation or transgender identity, should be reported to True Vision, which tackles all forms of hate crime. [True Vision](#) will give you information on content which indicates hatred and how to report it.

Media content inappropriate for children

If you want to make a complaint about an advert, television or radio programme, film, newspaper, magazine, video game or other type of content online or offline, that you think is unsuitable for children, you can report it using [ParentPort](#).

Getting help/advice

Many popular online services have some really useful help and advice areas, as well as ways to report and block content that is not allowed on the site (for exmple, cyberbullying).