

Longlevens Infant School
 Paygrove Lane,
 Longlevens,
 Gloucester,
 GL2 0AX
 Telephone: 01452 520061
 E-mail: infant@lpf.school



Longlevens Junior School
 Church Road,
 Longlevens,
 Gloucester,
 GL2 0AL
 Telephone: 01452 530177
 Email: junior@lpf.school

NAME OF POLICY:	Online Safety and Smart Device Policy
DATE OF APPROVAL:	March 2026 [sections 12 and 13 September 2026]
POST HOLDER RESPONSIBLE:	DSL (Designated Safeguarding Leads): Kate Hart & Becky Davis
GOVERNOR COMMITTEE OR INDIVIDUAL:	Safeguarding Link Governor
REVIEW DATE:	March 2027

CONTENTS

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Education
5. Training
6. Bring Your Own Device
7. Use of Digital Imaging and Video Images
8. Communications
9. Artificial Intelligence
10. Data Protection
11. Social Media and Website
12. Pupils Using Electronic and Smart Devices in School
13. Searching and Examining Electronic Devices (see also Behaviour Policy)
14. Unsuitable/inappropriate activities

Appendix 1	Acceptable Use Policy Agreement – Staff, Governor, Volunteer & Visitor
Appendix 2	Pupil Acceptable Use Agreement
Appendix 3	Parent/Carer Acceptable Use Agreement
Appendix 4	Responding to incidents of misuse – flowchart
Appendix 5	Unsuitable/Inappropriate activities
Appendix 6	Performance Photography & Filming Announcement



1. Aims

Longleaves Primary Federation aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole federation community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.



3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Executive Headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the federation has appropriate filtering and monitoring systems in place on federation devices and federation networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with service providers what needs to be done to support the federation in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the federation's ICT systems and the internet (appendix 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing a Federation approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Executive Headteacher



The Executive Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the federation.

3.3 The Designated Safeguarding Lead

Details of the federation's Designated Safeguarding Leads (DSL) and Deputy Designated Safeguarding Leads (DDSL) are set out in our safeguarding policy, as well as relevant job descriptions.

- The DSLs, as well as the Online Safety Lead, takes lead responsibility for online safety in school, in particular:
- Supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the federation
- Working with the Executive Headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on federation devices and federation networks
- Working with the network manager to make sure the appropriate systems and processes are in place
- Working with the Executive Headteacher, network manager, technical support and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the federation's safeguarding policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the federation's behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety across the federation to the Executive Headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 Network manager and technical support

The network manager and technical support are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on federation devices and federation networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially



harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the federation's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the federation's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the federation's ICT systems and the internet (appendix 1), and ensuring that pupils follow the federation's terms on acceptable use (appendix 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged on CPOMs using the Online Safety tag.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the federation's behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the Executive Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the federation's ICT systems and internet (appendix 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)



- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the federation's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

4. Education

Pupils

All schools have to teach [Relationships Education, Relationships and Sex Education \(RSE\) and Health Education](#); pupils will be taught about online safety as part of the curriculum.

Pupils in **EYFS and Key Stage (KS) 1** will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Parents/carers



The federation will support parents/carers to respond to incidences where their child has come across inappropriate or potentially harmful material on technology. The federation will therefore seek to provide information and awareness to parents and carers through:

- Letters, parents' evenings, website
- Parents/Carers will receive regular guidance on online safety issues through the federation newsletter.
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications e.g. www.swgfl.org.uk
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

The Wider Community

There may be occasions where members of the wider community gain from the federation's online safety knowledge and experience. This may be offered through the following:

- The federation website may provide online safety information for the wider community through this policy and other online safety messages as appropriate.

5. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing and misogynistic messages
 - Non-consensual sharing of making or sharing of nudes or semi-nudes and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term



The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

6. Bring Your Own Device (BYOD)

Children are not allowed to bring their own device to school for use in the classroom. Staff are permitted to bring their own device - see Appendix 1.

7. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. The federation will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Parents/carers use of digital and video images – see appendix for script and further information.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow federation policies concerning the sharing, distribution and publication of those images. Those images should only be taken on federation equipment; the personal equipment of staff should not be used for such purposes, unless staff have been given explicit permission to do so by a member of the Federation SLT.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the federation into disrepute.
- Pupils' full names will not be used anywhere on a website or social media pages particularly in association with photographs. Staff will not publish photos of any pupils whose parents have requested they are not, or where there will be legal or safety implications for the child (i.e.- CP/LAC)
- On entry to the school, permission will be obtained from parents/carers before photographs of pupils are published on the federation website or social media pages.
- To document children's learning in EYFS, Seesaw will be used as a platform for sharing learning with parents/ carers. On entry to school parents/carers will provide written permission for photographs of their child to be published.

8. Communications

The following table shows how the use of certain technologies has the potential to enhance/disadvantage learning:



	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons (*)		X						X
Use of mobile phones in social time	X							X
Taking photos on mobile phones				X				X
Use of other mobile devices e.g. tablets, gaming devices		X					X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X				X
Use of messaging apps		X						X
Use of social media			X					X
Use of blogs		X					X	

(* Access is permitted in order to obtain 2FA codes e.g. CPOMS or Microsoft 365)

When using communication technologies, the federation considers the following as good practice:

- The official federation email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to SLT or (if appropriate) Governance – in accordance with the federation policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Parents should communicate with staff in the first instance through the federation administration emails domain emails (infant/junior@lpf.school). Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information should not be posted on the federation website or social media accounts.

9. Artificial Intelligence

Artificial Intelligence (AI) refers to technology that can perform tasks that normally require human intelligence, such as recognising patterns, generating text or images, and answering questions. AI tools have rapidly developed in recent years and are now commonly found in everyday apps, search engines, and educational platforms used by children and staff.



The federation recognises that AI is evolving rapidly and whilst AI offers significant benefits for teaching and learning, it also raises important considerations around accuracy, privacy, ethics and safe use.

This section outlines how AI should be used responsibly within the school to support a safe and secure learning environment.

9.1 Staff

Staff may use AI tools to support teaching, planning, and workload management, but must do so in a safe, ethical, and compliant manner. Staff must:

- Only use Microsoft Co-Pilot (when logged in to their @lpf.school account) for any tasks involving personal information.
- Only use Microsoft Co-Pilot or Google Gemini for tasks which don't involve personal information.
- Check accuracy and appropriateness. AI-generated content may contain mistakes or biased information. Staff must critically review all AI outputs before using them in the classroom or communication.
- Use AI to enhance, not replace, professional judgement. AI may support lesson ideas, resources, or differentiation but should not be relied on for assessment decisions or pastoral matters.
- Never use AI 'live' in front of pupils.

9.2 Pupils

Presently, pupils will not be permitted to actively use AI in school, however we recognise that pupils will be exposed to AI at times, for example the Gemini result at the top of a Google search.

Pupils will be taught what AI is and about its reliability and accuracy within the general umbrella of discerning digital data.

10. Data Protection (see associated Data Protection policy)

Staff will ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software



- the data must be securely deleted from the device, in line with federation policy once it has been transferred or its use is complete

11. Social Media and Website

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff.

The federation provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the federation through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions are laid down in the federation's safeguarding and behaviour policies.

Federation staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or federation staff
- They do not engage in online discussion on personal matters relating to members of the federation community
- Personal opinions should not be attributed to the federation or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff should not invite children and young people (past or present) onto personal social networking sites or accept connection requests.

When using official federation websites there will be:

- approval given by senior leaders.
- Administration and monitoring of this account to ensure content is effective by website manager annually.

When using official federation social media accounts there will be:

- approval given by senior leaders.
- Administration and monitoring of this account will be carried out by website manager.
- Users of the account, will be familiar with systems for reporting and dealing with abuse and misuse and an understanding of how incidents may be dealt with under federation disciplinary procedures.

The federation's use of website and social media for professional purposes will be checked regularly by the SBM to ensure compliance with the policy.

12. Pupils and Personal Smart Devices in School

Longleaves Primary Federation is a (personal) smart-device-free environment for children. Pupils are not permitted to bring smart devices (this phrase refers to, but is not exclusive to smart phones,



smart watches, tablets and smart fitness bracelets) on to school grounds. A smart device is defined at Longlevens as an electronic device that can connect to the internet or other networks and can perform functions beyond its basic capabilities, often with the ability to interact with users and other devices. These devices typically include a microprocessor and can be found in various forms, from smartphones and wearables to smart appliances.

Pupils are permitted to have GPS tags and non-smart phones. Such phones must be handed to the class teacher for storage as soon as the child arrives in school. The phone will be returned to the pupil at the end of the school day. Such devices are usually brought to school by children arriving and leaving independent from their parent/guardian.

Non-smart mobile phones are not permitted to be used throughout the school day. In the event of a child attending an after-school club, the phone should be stored in the child's bag or handed to the adult facilitating the session, to be returned at the end of the club.

Children arriving late to school, for example if they have been at an appointment, should still hand their non-smart phone in to the class teacher for safe storage.

Where a child chooses not to hand non-smart mobile phone in to their teacher for safe keeping throughout the day, the mobile phone will be confiscated by the class teacher and kept safely until the school day has ended.

Where a child is found with a smart device on the school grounds, the device will be confiscated by an adult and held in the school office for collection by the child's parent/guardian. The parent/guardian will be contacted by a member of school staff informing them that the device has been confiscated and is available for parents to collect at the end of the school day.

The Federation takes no responsibility for the loss of or damage to any electronic device brought onto the school premises. This includes permitted and prohibited devices.

13. Searching and Examining Electronic Devices (see also Behaviour Policy)

The Head of School and any member of staff authorised to do so by the Head of School 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

Any time such a search is conducted, parents will be informed at the earliest available opportunity. 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 the most senior member of staff available
- 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

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation



- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

14. Unsuitable / inappropriate activities

The federation believes that the activities referred to in Appendices 4 and 5 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.



Appendix 1

Acceptable Use Policy Agreement – Staff, Governor, Volunteer & Visitor

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This AUP should be read in conjunction with the federation's safeguarding policies with particular regard for the Online Safety policy.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, ~~personal and recreational~~ use.
- that federation ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The federation will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

We recognise that federation devices are used at home, however they should be used in accordance with the AUP and any misuse will be subject to disciplinary procedures.

For my professional and personal safety:

- I understand that the federation will monitor my use of the ICT systems, email and other digital communications if necessary.
- I understand that the rules set out in this agreement also apply to use of federation ICT systems (e.g. laptops, email, remote platforms etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the federation ICT 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 by the federation.

We appreciate that there may be times when you need to access your personal email (these should be rare) during the school day.

- 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 understand that I should not write down or store a password where it is possible that someone may steal it.



- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using federation ICT 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 federation's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have explicit permission to do so from a member of Federation SLT.
- I will only communicate with pupils and parents/carers using official federation systems. Any such communication will be professional in tone and manner.
- The federation and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the schools.
- When I use my mobile devices (laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using federation equipment. I will also follow any additional rules set by the federation 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 avoid using personal email addresses on the federation ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (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 federation 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 internet 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 federation policies.
- I will not disable or cause any damage to federation 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 Federation/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data 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 federation 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.



When using the internet in my professional capacity or for federation sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I understand that this Acceptable Use Policy applies not only to my work and use of federation ICT equipment in school, but also applies to my use of federation ICT systems and equipment off the premises, as well as my use of personal equipment on the premises or in situations related to my employment by the federation.
- I understand that whilst my conduct online and use of personal ICT equipment and systems in my own time is not subject to this AUP, it could be addressed within the Federation Code of Conduct.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the federation ICT 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.

Staff / Volunteer Name:

Signed:

Date:



Appendix 2

Longlevens Infants School

Pupil Acceptable Use Agreement



Think then Click

These rules help us to stay safe on the internet.

We use them at school and at home.

- Only click on the buttons or links when we know what they do.



- Search the internet with an adult.



- Always ask if we get lost on the internet



- If we see something we don't like: In school and at home we turn off the screen and tell the person caring for us.

- Don't tell anyone our passwords or information about ourselves.



- Send and open emails or messages together.



- Know that not everyone using the internet tells the truth, so we must not make friends with people we don't know without telling our teachers or parents first

I understand the rules above and agree to follow them.

Reception:

Date:

Year 1:

Date:

Year 2:

Date:



Longlevens Junior School

Pupil Acceptable Use Agreement



This agreement will help keep me safe online:

1. ***I learn online*** – I use the school's internet and devices for schoolwork and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
4. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
5. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes addons can cost money, so it is important I always check for these too.
6. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
7. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
8. ***I never meet up with people I have met online*** - I know new online friends might not be who they say they are. I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
9. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it;
10. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
11. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.



12. ***I am private online*** – I do not share personal details such as my full name, my address, phone number, location or anything else that could identify me or my family and friends with people I don't know; if I turn on my location, I will remember to turn it off again.
 13. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even if I delete it).
 14. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
 15. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
 16. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
 17. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.
- ~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult, which includes:

My class teacher, Mrs Sharpe, Mrs Hart and Mrs Flattery.

Signed: _____ Date: _____



Appendix 3

Acceptable Use Policy Agreement – Parent/Carer

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Online Safety Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that federation systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The federation will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is available on the federation website, so that parents/carers will be aware of the federation expectations of the young people in their care.

I understand that the federation has discussed the Acceptable Use Agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the federation will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the federation cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be guided and that the federation will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the federation if I have concerns over my child's online safety.

Name:

Signed:

Date:



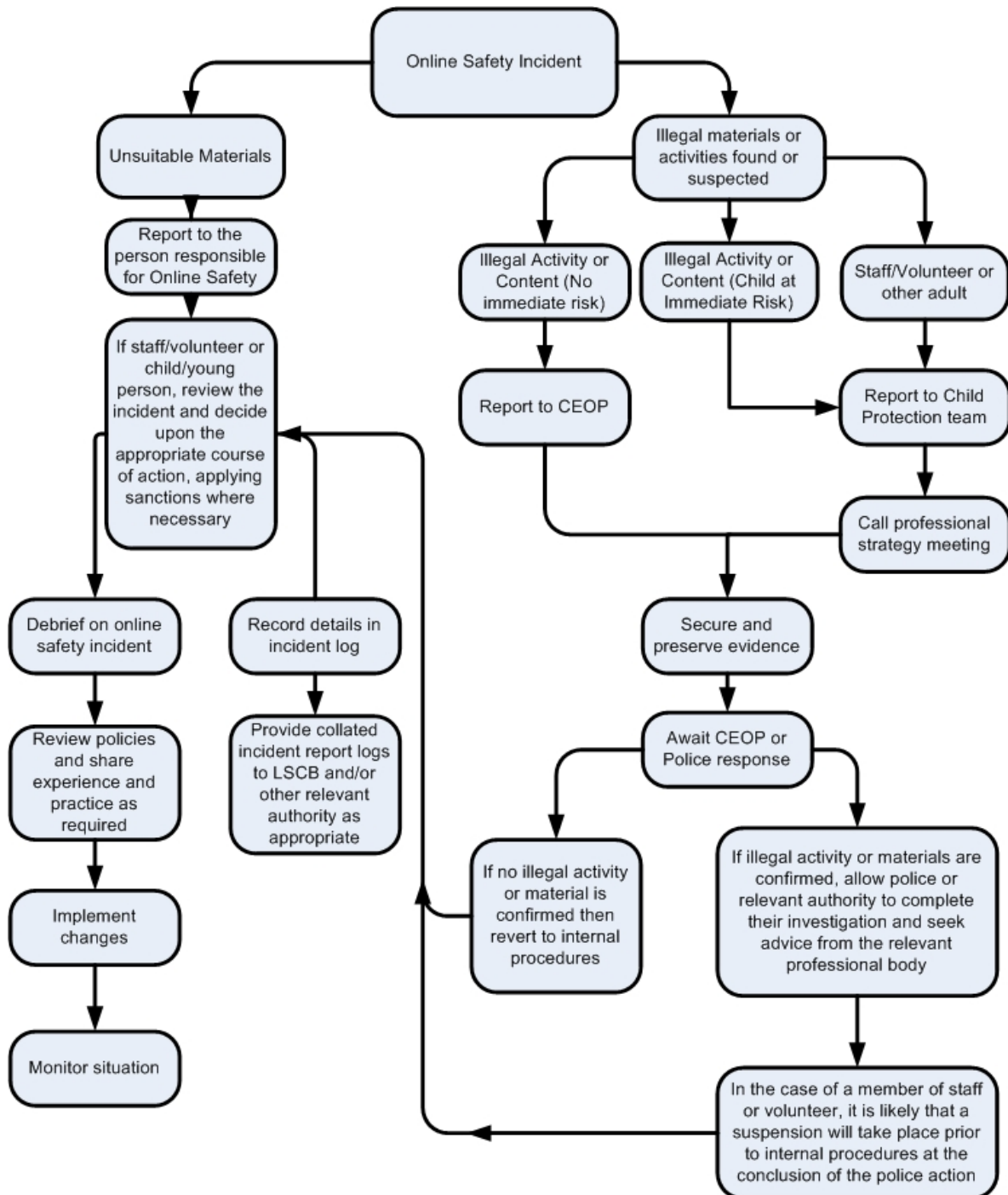
Appendix 4

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.





Other incidents

The federation hopes that all members of the federation community will be responsible users of digital technologies, who understand and follow federation policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure will be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure. It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by LADO or national/local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the federation and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Federation Actions & Sanctions

It is more likely that the federation will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the federation community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:



Appendix 5

Unsuitable / Inappropriate activities

(when using Federation ICT equipment, network and/or systems)

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Phase Lead	Refer to Head of school/ EHT	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal		X	X	X		X			
Unauthorised use of non-educational sites during lessons		X				X			
Unauthorised use of mobile phone / digital camera / other mobile device		X				X			
Unauthorised use of social media / messaging apps / personal email		X				X			
Unauthorised downloading or uploading of files		X				X			
Allowing others to access school / academy network by sharing username and passwords			X			X			
Attempting to access or accessing the school / academy network, using another student's / pupil's account			X			X			
Attempting to access or accessing the school / academy network, using the account of a member of staff			X			X			
Corrupting or destroying the data of other users			X			X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X			
Continued infringements of the above, following previous warnings or sanctions			X	X		X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X			
Using proxy sites or other means to subvert the school's / academy's filtering system			X			X			
Accidentally accessing offensive or pornographic material and failing to report the incident			X			X	X		
Deliberately accessing or trying to access offensive or pornographic material			X			X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X	X		



Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head of school/ EHT	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X	X					
Unauthorised downloading or uploading of files		X						
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		X						
Careless use of personal data e.g. holding or transferring data in an insecure manner		X						
Deliberate actions to breach data protection or network security rules		X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X						
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils / parents		X						
Actions which could compromise the staff member's professional standing		X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X	X					
Using proxy sites or other means to subvert the school's / academy's filtering system		X						
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material		X	X	X				
Breaching copyright or licensing regulations		X	X	X				
Continued infringements of the above, following previous warnings or sanctions		X	X	X				X



User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing		X				
Use of social media				X		
Use of messaging apps			X			
Use of video broadcasting e.g. YouTube			X			



Appendix 6 –

Performance Photography & Filming Announcement

Good [morning/afternoon] everyone, and a very warm welcome to [Longlevens Infant/Junior School].

We are so excited to have you here to share in the hard work and talent of our students.

Before we begin the performance, I have a vital request regarding photography and filming. We ask that you please refrain from taking any photos or video recordings during today's event.

While we completely understand the desire to capture these precious memories, we have a significant number of children in our school community for whom we do not have parental or legal consent to be photographed or recorded. In many cases, this is a critical safeguarding requirement to ensure the privacy and safety of our pupils.

We live in an increasingly litigious society, and as a school, we want to respect the wishes of you our parents in terms of permissions and of every child in our care. Distributing images on social media, even unintentionally, can lead to serious legal and safeguarding complications for both the school and individuals.

To ensure you still have a memento of the day, we [will be taking a group photo of the cast / will provide a photo opportunity at the end with your own child only].

We appreciate your cooperation in helping us keep all our students safe and allowing everyone to enjoy the performance through their own eyes rather than a screen.

Thank you for your understanding.