

Littleport Community Primary School and Preschool



Littleport Community
Preschool



ONLINE SAFETY POLICY

Ratified: November 2025

Review: November 2026

Signed: 

Chair of Governors

Date: 27th November 2025

Online Safety Policy

Contents

- 1. Background.....3
- 2. Rationale.....4
- 3. The Online Safety Curriculum.....5
- 4. Continued Professional Development.....6
- 5. School Website.....7
- 6. Monitoring, and Preventing Online Safety Incidents.....7
- 7. Responding to Online Safety Incidents.....8
- 8. Artificial Intelligence (AI).....12
- Appendices (including AUPs)

1. Background

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding to online safety incidents
- A progressive, age appropriate online safety curriculum for all pupils, which meets the requirement of the National Curriculum for Computing and the statutory Relationships and Health Education

Online safety in schools is primarily a safeguarding and not a technology one. Therefore, this policy should be viewed alongside other safeguarding policies and approaches including, but not limited to:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff at induction
- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Cambridgeshire Progression in Computing Capability Materials
- Whistle Blowing Policy
- **Artificial Intelligence (AI) Policy**

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices (AUPs). These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our safety policy involved:

- The Headteacher
- The Designated Safeguarding Lead
- Online safety Leader
- The Computing Subject Leader
- Cambridgeshire Education ICT Service
- The Governor responsible for Safeguarding

This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via email and a staff meeting and is readily available on the school network and website.

All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As online safety is an

important part of our school's approach to safeguarding, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

2. Rationale

At Littleport Community Primary School we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the 4 C's; **Contact, Content, Conduct, and Commerce** (*Keeping Children Safe in Education, 2025*) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of self-generated indecent images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Phishing or financial scams
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops and also desktops in the office, Site Manager's office and **Children's Inclusion Manager's office**; laptops including staff level internet access; server access and access to Management Information Systems (MIS)
- Some staff have access to school systems beyond the school building (e.g. MIS systems, cloud platforms e.g Microsoft 365/Teams). Staff laptops can also be used at home in accordance with the staff AUP
- Governors and visitors also have access to the internet and can use the facility in accordance with the associated AUP

- Curriculum iPads for preparing and delivering pupil activities
- Class cameras and other peripherals such as visualisers and interactive whiteboards

Pupils:

- Curriculum iPads, laptops from the trolley and locations across the school including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, Makey Makeys, control equipment, class cameras etc.)
- Cloud platforms (Microsoft Teams)

Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

3. The Online Safety Curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the [National Curriculum for Computing \(England\)](#) and the statutory [Relationship and Health Education](#).

At Littleport Community Primary School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials
- Our programme for online safety education is evidenced in teachers' planning either as discrete or embedded activities
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments
- Key online safety messages are also delivered and reinforced through termly whole school assemblies focusing on different themes pertinent to the school
- A flexible curriculum which is able to respond to new challenges as they arise
- A partnership with parents/carers with an aim to inform and support them with online safety at home

In Key Stage (KS1), pupils 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 (KS2) 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

- Be discerning in evaluating digital content

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

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- 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, 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 are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- 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 benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

4. Continued Professional Development

In accordance with KCSiE guidance, staff at Littleport Community Primary School receive safeguarding and child protection training at induction. This training covers online safety, which amongst other things, includes an understanding of expectations, applicable roles and responsibilities in relation to filtering and monitoring. Safeguarding, child protection and online safety training is regularly updated during staff meetings and through updates from the school's

online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

The Online Safety Lead/Designated Safeguarding Lead and the link safeguarding governor are responsible for ensuring the DfE filtering and monitoring standards are met. These nominated members of staff receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

New staff receive information on the school's Acceptable Use Policy as part of their induction, including advice on protecting their professional reputation online.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

5. School Website

The main purpose of our school website is to provide information. Our school website not only tells the world that our school exists, but it provides information for our pupils and parents, promote the school to prospective ones and publish the statutory information required by the Department for Education.

In conjunction with a range of online services, our school website is used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and share resources for teaching and learning both within the school and with colleagues elsewhere as well as parents and carers at home.

Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as it would apply to its physical surroundings. Headteachers and the Governing Body, therefore, take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, a visitor using the school website.

The school has established clear practice to ensure that its website is maintained, is effective, and does not compromise the safety of the pupils or staff.

6. Monitoring and Averting Online Safety Incidents

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by The ICT Service on behalf of the Local Authority. Safeguards built into the school's infrastructure include:

- Secure, private **BTnet** internet connection to each school with a direct link to the **Joint Academic Network (JANET)**. This is provided and maintained by the **Joint Information System Committee (JISC)** as well as **The ICT Service** on behalf of the local authority.

- Managed firewalling running Unified threat management (UTM) that provides restrictions on download of software, apps and file types from known compromised sites
- Foundation DDoS mitigation service, security analysts carefully monitor the patterns of traffic across the network
- Enhanced web filtering provided by **Netsweeper** to all sites as standard
- Optional SSL decryption available on web traffic to allow for greater visibility of sites being accessed and requested
- Prevention of devices and network accessing known malicious or compromised domains provided by **Janet Network Resolver Service (JNRS)**
- Antivirus package provided as part of **JISC package**

Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- Appropriate levels of supervision when pupils are using online technologies
- Auto-generated alerts which flag up activity in specific safeguarding categories which may raise child protection concerns
- Use of additional reporting tools to monitor and investigate pupil use of the internet and school provided devices

Staff use of the schools' internet **is** also monitored and investigated where needed.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network, which are changed regularly
- Governors have their own secure access to emails as part of the school's network and Governor section on the school website and Microsoft Teams, which are accessed via a separate log in.
- Visitors/Supply teachers can access part of the network using a generic visitor login and password
- The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office and Online Safety Leader
- School staff and pupils are not permitted to connect personal devices to the school's wireless network unless permission is granted by the Headteacher

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

7. Responding to Online Safety Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.

If an online safety incident occurs, Littleport Community Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendices- or reporting incidents to the police and other authorities). See separate policy for staff AUP.

In addition, the Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

With this in mind, the Headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if they deem it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents (where appropriate) before taking any further action.

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

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

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 a member of the Designated Safeguarding Team
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Designated Safeguarding Lead and/or Deputy Designated Safeguarding Lead to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carers refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

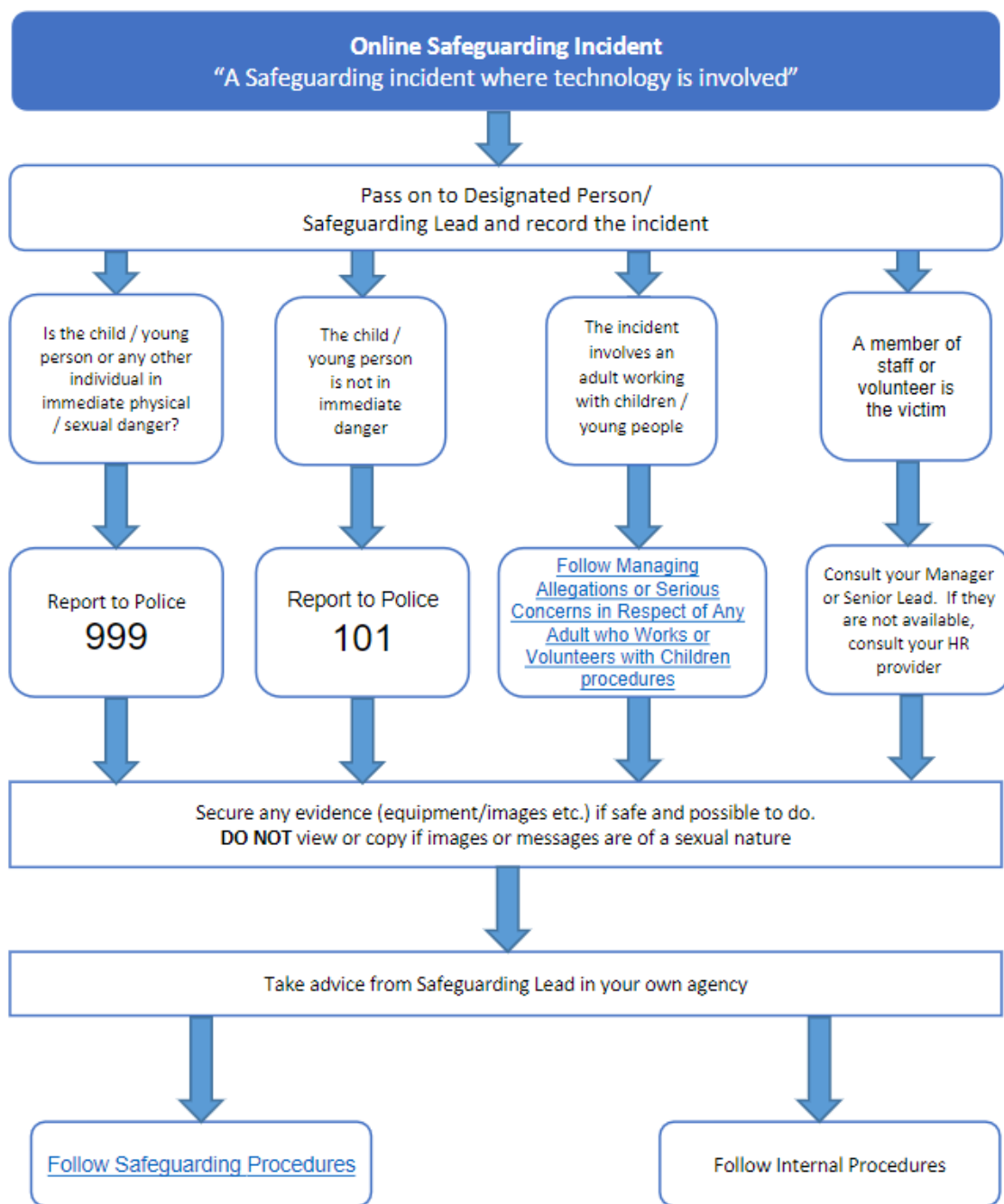
- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure

NB: In our school, the likelihood of these types of instances occurring are already reduced as we do not allow pupils to use personal devices in school. They are instead handed in at the office in the morning and collected at the end of the school day. Children are not permitted to wear 'smart' watches for safeguarding reasons. These measures also restrict their access to 3G, 4G and 5G networks in school.

Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed. This process is illustrated in the diagram below. **All online safety incidents will be logged as a safeguarding concern using the school's electronic reporting system, MyConcern.**

You come across a Safeguarding concern involving technology ...



Throughout this process, please ensure that all those involved are supported appropriately

If you think that a child or young person is at risk of serious harm contact Children Social Care

<https://safeguardingcambspeterborough.org.uk/concerned/>

Out of hours emergencies 01733 234724.

8. Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Littleport Community Primary School and Preschool recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Littleport Community Primary School and Preschool will treat any use of AI to bully pupils very seriously, in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of AI should be carried out in accordance with our AI Policy.

Appendix 1 Pupil AUPs



Littleport Community Primary School EYFS Acceptable Use Policy



Tell a parent or adult if you are using the Internet.



Don't tell anyone your password.



Do not give out personal information.



Do not send anyone a photo of you, your family or friends.



Tell an adult if you see anything worrying on the computer.

Pupil's name: _____

Pupil's signature: _____

Date: _____



Littleport Community Primary School KS1 Acceptable Use Policy

- I will only use the school's ICT equipment and tools (including computers, cameras etc.) for schoolwork and home learning. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the internet and email when an adult is nearby.
- I will not share my passwords with other people and will tell my teacher if I think someone else knows them.
- I will ask an adult before opening **communication** from someone I don't know.
- I will not share details about myself, such as surname, phone number or home address.
- I will ask if I need to look at other peoples' work on the computer.
- I will try my hardest to only send messages which don't upset other people.
- I will ask my teacher before using photos or video.
- If I see something on a screen which upsets me, I will always tell an adult.

I will do my best to follow these rules because I know they are there to keep me and my friends safe. If I don't follow these rules, I know that my teacher may stop me using technology at school and / or talk to my parents about how I use technology.

Pupil's name: _____

Pupil's signature: _____

Date: _____



Littleport Community Primary School KS2 Acceptable Use Policy

- I will only use the school's ICT equipment and tools (including computers, cameras etc.) for schoolwork and home learning. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the Internet if an adult is in the room with me.
- I will only delete my own files unless my teacher gives me permission to delete someone else's. I will not look at other people's files without their permission.
- I will keep my passwords private and tell an adult if I think someone else knows them. I know that my teacher can change my passwords if needed.
- I will only open e-mail attachments from people who I know or an adult has approved. If I am unsure about an attachment or e-mail, I will ask an adult for help.
- I will not give my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends or my family. If I have to use an online name I will make one up!
- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.
- I will never arrange to meet someone I have only ever previously met online. It could be dangerous.
- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I find anything via Internet, e-mail or mobile phone that is upsetting or makes me feel uncomfortable, I will tell a teacher or responsible adult.
- I will not use AI tools and generative chatbots:
 - During assessments
 - To present AI-generated work (text or imagery) as my own

I will do my best to follow these rules because I know they are there to keep me and my friends safe. If I don't follow these rules, my teacher or **Online Safety Lead** may:

- Speak to me about my behaviour.
- Speak to my parents about my use of technology.
- Remove me from communities or groups.
- Turn off my community / group accounts for a little while or permanently.
- Not allow me to use laptops / computers to access the internet or particular programmes.
- Take other action to keep me (and others) safe.

Pupil's name: _____

Pupil's signature: _____ Date: _____

LCPS Visitor ICT Acceptable Use Policy



Acceptable internet usage policy and disclaimer for individuals not employed by the school accessing using the School's Internet access including Wi-Fi provision.

This policy supplements any school Online Safety and Acceptable Use Policies that users must comply with.

You are recommended to ensure you are familiar with, and understand the content of these policies. You are advised that all work undertaken using the Internet and Wi-Fi service is monitored and logged, not only for this purpose but also to allow monitoring of service provision.

In particular, you **must not** and by using the service you **agree not to**:

- Access network services in such a way as to deny reasonable access to the network for other users, for example, by excessive use of network bandwidth. This could include the use of FTP servers, file-sharing software and video streaming
- Download any images, text, sound or other material that is in breach of copyright. The School accepts no responsibility for any breaches that may occur.
- Deliberately visit, view or download any material from any website containing pornographic, abusive, racist, violent or illegal material or material which is offensive in any way whatsoever. The School's decision as to which websites fall into these categories is final.
- Upload or make available to others any material that is offensive, obscene, indecent, or which infringes the copyright of another person (e.g. images, audio and video files).
- Use School printing services without prior approval from the school.
- Use the Internet for any illegal activity or gambling.
- Use the Internet to harass, cause annoyance, inconvenience or anxiety to others.
- Access, or attempt to gain access to, computer systems, data or resources to which they are not authorised, such as connecting to other user's resources. By using the service you agree to respect the privacy of others.
- Share further any network credentials obtained to connect to our network
- Attempt to gain unauthorised access to restricted part of the network, or attempt to undermine the integrity or security of any computer systems or network. You, the user, are responsible for any damage caused to the computer equipment arising out of any wilful act or negligent misuse.

Breach of the above will lead to users being banned from using the service and may result in prosecution. The School reserves the right to update or modify the above terms at any time without prior notice.

Your use of the service following any such change constitutes your agreement to follow and be bound by these terms as modified.

Disclaimer 1. Service provided "as is". This service provides access to the Internet on an "as is" basis with all risks inherent in such access. 2. Service provided "as available". The service is provided on an "as available" basis without warranties of any kind, either express or implied. 3. Indemnity. The School assumes no responsibility for damages, direct or indirect from its connections to the internet, nor for the accuracy and effectiveness of any installed filter. The School cannot be held liable for any information that may be lost, damaged, stolen or unavailable due to technical or other difficulties. The School is not responsible for the configuration of any personal equipment or changes to these resulting from connection to the School's network. It is the sole responsibility of users to provide anti-virus protection, personal firewall protection and to configure their device's (laptop or other equipment) settings to provide the appropriate security settings to control access from other wireless devices within the range of the School's Wi-Fi service and the Internet itself.

Signed:

Name:

Dated:

School contact: Mr Adam Rivett
(Headteacher & Online Safety Lead)