Laxton Junior School
OUNDLE

Online Safety Policy

The Corporation of Oundle School includes both Oundle School, a boarding and day School for pupils aged 11 – 18 and Laxton Junior School, a day School for pupils aged 4 - 11. This policy applies solely to Laxton Junior School.

Introduction and Aims

Technology has become a fundamental part in the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet is an incredibly powerful tool, which can open up new opportunities for everyone. Communication through technology helps teachers and pupils learn from each other and this can stimulate discussion, increase creativity and promote effective learning. The use of exciting and cutting-edge technology in school and at home has been shown to raise educational standards and boost pupil achievement. In order to magnify these opportunities, children and young people should have safe internet access at all times.

Our school aims to:

- Create a safe and secure environment for children to use technology.
- Have a curriculum in place that ensures safe and appropriate use of technology throughout the school.
- Have procedures in place to identify and intervene should any online safety issues occur.

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping children safe in education, and its advice for schools on:

- Teaching online safety in schools.
- Preventing and tackling bullying and cyberbullying: advice for head teachers and school staff.
- Searching, screening and confiscation.
- Harmful online challenges and online hoaxes.
- Filtering and monitoring. `

It also refers to the Department for Education'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 cyberbullying 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.

In the statutory guidance, it states that Online safety can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful material; for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism
- **Contact**: being subjected to harmful online interaction with other users; 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 (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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

Roles and Responsibilities

Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Head to account for its implementation.

The Governing Body should:

- Attend regular meetings with the Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL) to discuss online safety and monitor online safety incidents as provided by the DSL and DDSL
- Approve this policy and review the effectiveness of it
- Ensure that filtering and monitoring provision is reviewed and recorded, at least annually
- Agree and adhere to the terms on acceptable use of the school's Information Technology (IT) systems and the internet

The Governing Body member who over sees Safeguarding, including online safety, is: Suzanna D'Oyly.

Head

The Head should:

- Ensure a duty of care for the safety of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Be responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. This is delegated to the Designated Safeguarding Lead (DSL).

Online Safety Lead (Deputy Designated Safeguarding Lead)

The Online Safety Lead should:

- Ensure that staff understand this policy and that it is being implemented consistently throughout the school.
- Create and regularly update an Online Safety Curriculum that builds resilience and future proofs the children with skills that will be important throughout their time at Laxton Junior School and beyond.

- Meet regularly with Designated Safeguarding Lead to discuss Online Safety updates throughout the school.
- Be a member of the Oundle School Online Safety Group and attend meetings.
- Ensure annual online safety training to provide staff with relevant skills and knowledge.
- Ensure that staff receive regular training (for example, via email, briefing notes, e-bulletins and staff meetings) on online safety, allowing them to stay up to date with any developments,
- Give regular Online Safety updates during staff briefing.
- Work with the DSL and other staff, as necessary, to address any online safety issues or incidents.
- Ensure that any incidents of cyberbullying are logged and dealt with appropriately in line with the relevant policies.
- Liaise with other agencies and/or external services if necessary.
- Work with the Head of IT and Information Management on all aspects of filtering and monitoring.
- Provide regular reports on online safety in school to the Head and Governing Body.
- Be responsible for receiving reports of online safety incidents and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.

Designated Safeguarding Lead

The DSL should support the Online Safety Lead in all aspects of their role, including but not limited to:

- Ensuring all staff understand the online safety policy and implement it throughout the school.
- Ensuring all online safety issues are logged and dealt with appropriately.
- Ensure online safety training is given to all new staff as part of their induction.
- Regularly updating the online safety curriculum.
- With support from the Head of IT and Information Management and Deputy DSL, implement all aspects of filtering and monitoring throughout the school.
- Keeping staff informed and updated with any developments on online safety.
- Be responsible for receiving reports of online safety incidents and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.

Head of IT and Information Management and IT Department

The Head of IT and Information Management and IT department should:

- Put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact whilst online at school, including terrorist and extremis material.
- Maintain the filtering and monitoring systems.
- Ensure the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conduct a full security check and monitor the school's ICT systems on a regular basis, in order that any misuse / attempted misuse can be reported to the Head Teacher or Online Safety Lead to investigate.
- Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files.
- Ensure that the school meets required online safety technical requirements and any Online Safety Policy / Guidance that may apply.
- Ensure users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- Ensure that monitoring software / systems are implemented and updated as agreed in school policies.

- Provide the Online Safety Lead with a daily and weekly filtering and monitoring report.
- Identify risks and share them with the Online Safety Lead.

Computing Lead

The Computing lead should:

- Have overall ownership of the Computing curriculum, including areas of online safety.
- Discuss and create the online safety curriculum with the Online Safety Lead.
- Monitor and evaluate the delivery of the online safety curriculum to all pupils through computing.
- Support the Online Safety Lead to ensure that online safety teaching is embedded in all aspects of the curriculum.

Computing Teachers

Staff teaching Computing should:

- Deliver the online safety curriculum to all pupils.
- Give feedback to the Online Safety Lead regarding all online safety matters.
- Ensure pupils know, understand and are adhering to the LJS Pupil Online Safety Charter in lessons.

All Staff and Volunteers

All staff and volunteers should:

- Promote online safety.
- Read and implement the Online Safety Policy throughout the school.
- Ensure online safety issues are embedded in all aspects of the curriculum.
- Adhere to the Staff Acceptable use of IT Policy.
- Work with the DSL and DDSL to ensure any online safety issues are logged.
- Ensure all issues regarding online bullying are dealt with appropriately and in line with the Countering Bullying and Cyberbullying Policy.
- Adhere to the Communications Policy and Photography, Filming and Publication Policy.

Pupils

All pupils should:

- Read and understand the LJS Pupil Online Safety Charter.
- Adhere to the LJS Pupil Online Safety Charter.
- Support their peers regarding all online safety matters and encourage them to make the correct choices when using technology.

Parents and Guardians

Parents and Guardians should:

- Support the school in promoting good online safety practice.
- Follow the Photography Privacy Notice.
- Follow guidelines on the appropriate use of the parents' sections of the website.
- Notify a member of staff or the Online Safety Lead with any concerns or queries linked to this policy or online safety.
- Ensure their child has read, understood and agreed to the school's Pupil Acceptable Use Policy.

Visitors

Visitors should:

- Check with a member of staff before using the school WiFi and to gain access via visitor passwords.
- Be made aware of this policy before using the school's IT systems or internet.
- Be aware and follow the Cameras and Mobile Phones Policy and Photography, Filming and Publication Policy. Information for visitors is within the Visitors' Information leaflet.

Educating our Community

Pupils

Online Safety is taught discretely as well as embedded into our curriculum and incorporates the use of relevant national initiatives and opportunities eg: Safer Internet Day and Anti-bullying Week.. It is this approach that ensures pupils' knowledge of how to keep themselves safe online, inside and outside of school, is as strong as possible. The curriculum will make pupils aware of some of the threats they may face, inside and outside of school, including but not limited to:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by people they have met online.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyberbullying.
- Access to unsuitable video / internet games.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Harmful online challenges and online hoaxes.

The curriculum will also give the children resilience and skills that they can use beyond their time at Laxton Junior School to protect themselves and their peers by encouraging them to:

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

The needs and progress of each learner is addressed through effective planning and assessment. Each year group, from Years 3 to 6, will be given a questionnaire to complete during the year and this will be analysed by the Safeguarding Team. Staff will be informed about what the children are being taught in an annual staff meeting and throughout the school year from the Online Safety Lead. Staff can then reinforce this content when they are using technology with the children. The curriculum is accessible to learners at different ages and abilities, including those with SEND. Vulnerability is actively addressed as part of a personalised online safety curriculum eg: victims of abuse.

By the end of their time at Laxton Junior School, pupils should know:

- How to use technology safely, respectfully and responsibly.
- 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.
- To recognise acceptable/unacceptable online behaviour.
- To keep personal information private.
- How information and data is shared and used online.

- That people sometimes behave differently online, including by pretending to be someone they are not.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, 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 to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff members will receive training as part of their induction on safe internet use and online safeguarding including cyberbullying and the risks of online radicalisation; staff will be provided with links to this policy and Acceptable Use Policies / Charters.
- All staff will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example: briefings, e-bulletins, online safety newsletter, staff meetings).
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/briefings.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.

Governors

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

Parents

The school is committed to raising parents' awareness of internet safety and will provide information and to parents and carers through:

- Letters and Newsletters.
- Parents/Carers in Partnership Sessions.
- High profile events e.g. Safer Internet Day.
- Providing further information through relevant web sites and external leaflets.
- Make clear how parents should report any concerns or worries.

Volunteers

Volunteers will receive appropriate training and updates, as applicable.

Acceptable Use Policies

The Acceptable Use Policies set out the security, administration and internal rules to be observed when communicating electronically or using the IT facilities provided by Oundle School. Staff and pupils should familiarise themselves with the terms of this Policy to minimise potential damage to them, other members of staff or pupils and the School, which may arise because of misuse of email or Internet facilities.
Please see Appendix 1 for the Pupil Acceptable Use Agreement named LJS Online Safety Charter.

Mobile and Smart Technology

Pupils at Laxton Junior School are not permitted to bring mobile phones or smart technology with 3G, 4G, or 5G connectivity onto school premises. This policy aims to ensure that children do not have unlimited and unrestricted access to the internet via mobile networks during school hours.

If a pupil requires a mobile device for a specific purpose, such as for walking home after school, parents must contact the school in advance. In such cases, the device will be securely stored in the front office for the duration of the school day.

Watches with pedometer functions are permitted.

School Use of Social Media

All staff should adhere to the Social Media Policy, available via The Staff Handbook.

Safer Internet Day

During our Safer Internet Day, the school runs a number of activities for the pupils, staff and parents. For the pupils, there are age-appropriate assemblies where the children will be reminded of how to stay safe online and focus on the annual theme. Throughout the week, the pupils will also focus on a specific area of online safety in their Computing lessons.

Linked to Safer Internet Day, staff professional development is planned and led by the Online Safety Lead. The school also holds a Parents in Partnership session for parental education.

Digital Leaders

Digital Leaders is a leadership opportunity for pupils in Years 5 and 6 linked to Online Safety. The group meets regularly with the aim of:

- Producing and delivering assemblies about online safety.
- Promoting the acceptable use of devices.
- Demonstrating how to use new apps or programs.
- Organising Safer Internet Day.
- Trying out and reviewing new apps, websites and programs which could be used in lessons.

Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- Clear reporting routes are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with Whistleblowing, Complaints and Managing Allegations policies.
- All members of the school community are made aware of the need to report online safety issues/incidents via CPOMS or by directly reporting to the DSL or DDSL.
- Reports will be dealt with as soon as is practicably possible once they are received.
- The DSL and DDSL have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures. This may include:

    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft of piracy
- Any concern about staff misuse will be reported to the Head, unless the concerns involved the Head, in which case the complaint is referred to the Chair of Governors and the Local Authority.
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
- One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise.
    - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recoded.
    - Record the URL of any site containing 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 any referral.
- Once this has been completed and fully investigated, the group will need to judge whether this concern meet the threshold to refer.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues eg: local authority, police, online safety helpline, CEOP
- Learnings from the incident (or pattern of incidents) will be provided to:
- Online Safety Group for consideration of updates to policies or education programmes and to review effective practices.
- Staff, through regular briefings.
- Learnings, through assemblies/lessons.
- Parents, through newsletters, school social media, website.
    - Governors, through regular safeguarding updates
    - Local authority / external agencies, as relevant
- Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Acceptable Use, Behaviour and other relevant policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Minor incidents may be dealt with solely by the Form Teacher or Online Safety Lead. More serious issues may be referred directly to the Designated Safeguarding Lead or Head.

Remote Learning

Where children are being asked to learn online at home, our Safeguarding Policy, this policy and any linked and/or relevant policies remain in place.

Monitoring Arrangements

CPOMS

Staff report and log concerns of incidents regarding behaviour and safeguarding issues related to online safety on CPOMS. The DDSL and DSL are alerted and respond to these appropriately. Regular meetings are held between the DDSL and DSL to discuss new incidents and review actions. The Head is informed of any relevant incidents by the DSL.

Knowledge

Monitoring of the pupils' online safety knowledge is done throughout the year during Computing lessons. As online safety learning outcomes are embedded through the Computing curriculum, we regularly assess pupil knowledge. An annual questionnaire is also given to pupils in Years 3 to 6 to monitor their online safety knowledge and allow them to voice any concerns they may have. This is done via whole class discussion in the Pre-Prep. The information taken from these processes is then used to help adapt, where needed, the online safety curriculum. Any concerns identified during these processes are reported, via CPOMS.

Teaching and Learning

The teaching of online safety through the Computing curriculum and Learning for Life is monitored by the Computing Lead and DDSL as part of their annual monitoring and review process and as part of the CPD and Appraisal process, where appropriate.

Staff knowledge is monitored through annual online safety training sessions. Regular updates linked to online safety are given throughout the year.

Filters, Informational Security and Access Management

The Head of IT and Information Management ensures that appropriate filtering and monitoring, information security and access management systems are in place. Filters limit children's exposure to risk from the school's IT systems.

The Head of IT and information Management is responsible for:

- maintaining filtering and monitoring systems
- reviewing the effectiveness of the provision
- completing actions following concerns or checks to systems
- technical security (Appendix 3)

Daily reports are run to identify inappropriate usage by users, including radicalisation and self-harm. These reports are sent through to the Deputy Designated Safeguarding Lead who will respond accordingly based on the content.

The Designated Safeguarding Lead and Deputy Designated Safeguarding Lead work closely with the Governors, and Head of IT and Information Management in all aspects of filtering and monitoring.

Filtering

- The schools manages access to content across its systems for all users on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE filtering standards for schools and colleges.
- Illegal content is filtered by the broadband or filtering provider.
- There are established a effective routes for users to report inappropriate content, recognising that no system can be 100% effective.

- There is a clear process in place to deal with, and log, requests / approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the DSL/DDSL to breaches of the filtering policy, which are then acted upon.

Monitoring

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the DSL/DDSL.
- All users are aware that the network (and devices) are monitored.
- There are effective procedures in place to report abuse/misuse.
- Management of serious safeguarding alerts in consistent with the Safeguarding policy

The filtering and monitoring provision is reviewed at least annually. The review is conducted by the Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL), and the Head of IT and Information Management, and should involve the Governor with responsibility for Filtering and Monitoring.

The review informs:

- Documenting decisions on what is blocked or allowed and why.
- Related safeguarding or technology policies and procedures.
- Roles and responsibilities.
- Training of staff.
- Curriculum and learning opportunities.
- Procurement decisions.
- How often and what is checked.
- Monitoring strategies.

Policy

This policy will be reviewed every year by the Online Safety Lead. At every review, the policy will be shared with the LJS Governing Body Subcommittee, including the Safeguarding Governor.

Personal Data

Personal data is managed in line with statutory requirements. Please see the Data Protection Policy for further details.

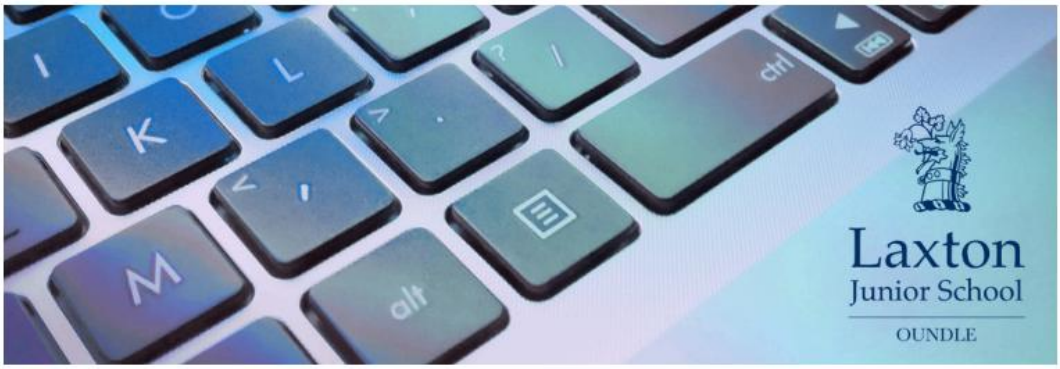
Linked Policies

This policy should be read in conjunction with:

- Safeguarding Policy
- ICT Staff Acceptable Use Policy
- ICT Pupil Acceptable Use Policy
- Social Media Policy
- Countering Bullying and Cyberbullying Policy
- Bring Your Own Device Policy
- Data Protection Policy
- Behaviour and Exclusion Policy

Reviewer	Fraser Harper
Post of Reviewer	DDSL & Online Safety Lead
Review Date	Michaelmas 2024
Approved by Governing Body	Michaelmas 2024
Reviewed and filed with both Schools	Michaelmas 2024
Next Review (max 3 years)	Michaelmas 2025

Appendix 1: Pupil Acceptable Use Policy



LJS PUPIL ONLINE SAFETY CHARTER

The LJS Pupil Online Safety Charter is based on the 4C's of online safety: content, contact, conduct and commerce. The charter was created by our Digital Leaders to help keep all pupils safe.

As part of the LJS community I agree to:

Passwords and Logins

- Keep my password safe and secret.
- Create a username that does not give away too much information about myself and a password that only I will know.
- Sign out when I am finished on my device.
- Lock my computer if I leave the room.
- Only use a computer that is logged in with my username and password.

Email and Messaging

- Not share my email address outside of the school community without permission.
- Only send messages related to school when using my school email account.
- Be polite and friendly in the messages I send.

School Work and Prep

- Not copy work from others or the internet
- Reference the websites I have used to help me with my work.

Web Browsing

- Only register my details on websites with permission.
- Only go to websites that are suitable for school.
- Tell my teacher if I see something inappropriate.
- Check that the websites I visit contain reliable information by checking on other websites.
- Not click on adverts.

Mobile Devices

- Only bring in mobile devices with permission from a teacher.
- Not bring in phones, smartwatches and gaming devices.
- When taking or sharing someone's photo, always ask permission first.

Remember, speak out to a trusted adult if you feel unsafe or worried.

Appendix 2: Online Safety Risks Information

Cyberbullying

Cyberbullying is a form of bullying or harassment by electronic means. It has become more and more prevalent in the last few years due to the introduction of various forms of social media.

Through the Online Safety curriculum, the pupils will be made aware of the seriousness of Cyberbullying and what to do when it occurs. Any form of bullying or harassment using emails, social media or message boards will be dealt with using the school Countering Bullying and Cyberbullying Policy.

Harmful Online Challenges and Online Hoaxes

A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

When a harmful online challenge or online hoax is circulating between children at Laxton Junior School, the local community or more widely we will undertake a case-by-case assessment, establishing the scale and nature of the possible risk to children at LJS, including considering (where the evidence allows) if the risk is a national one or is it localised to our area, or even just our setting. Quick local action may prevent a local online hoax or local harmful online challenge going viral (quickly and widely spread).

Staff should share their online safety concern via CPOMS or directly with the Online Safety Lead. Forward planning, together with case-by-case research, will allow for a calm and measured response and avoid creating panic or confusion.

We should continue to focus on what good online behaviour looks like, what we do if children see something upsetting online and who and where to report it. Staff should fact check with the Online Safety Lead, as this may help dispel myths if children are identifying that they are particularly concerned that the latest online challenge or online hoax has put them or their friends at risk.

Online Relationships

An online relationship is a relationship between people who have met online, and in many cases know each other only via the internet. Online relationships are similar in many ways to pen pal relationships.

There are possible danger present in online relationships. The option for an individual to conceal their identity may be harmless in many cases, but it can also lead to extremely dangerous situations. Hidden identities are often used in cases of cyberbullying and cyberstalking. Concealing a person's true identity is also a technique that can be used to manipulate their new online friend or lover into convincing them that they are someone completely different. This is something most online predators do in order to prey on victims.

Misleading Online Identities

There is a difference between keeping our identity private online and deliberately deceiving people. It is not OK to impersonate someone else to deceive or bully another person. Sometimes people do mislead people into thinking that they are someone else, for example by: creating a false profile eg: using someone else's photograph and false details such as age or gender, or pretending they know you, or your friends or family.

Online Information

There is a difference between keeping our identity private online and deliberately deceiving people. It is not OK to impersonate someone else to deceive or bully another person. Sometimes people do mislead people into thinking that they are someone else, for example by: creating a false profile eg: using someone else's photograph and false details such as age or gender, or pretending they know you, or your friends or family.

Sharing nudes and semi-nudes

In the latest advice for schools and colleges (UKCIS, 2020) this is define as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. If an incident comes to your attention you should act in line with the School's Safeguarding Policy and report it to the DSL or DDSL immediately.

Harmful Content

Harmful content generally involves information, images or videos that can be upsetting, misleading, promote dangerous behaviours or are directed at adults. This could include:

- Violence (for example, graphic images or videos).
- Adult sexual content and pornography.
- Misinformation (for example, misleading or dangerous information that can promote harmful behaviours).
- Hate (for example, promotion of extreme view or hate towards groups).
- Non-consensual sharing (for example, private images or videos shared with a wide audience).
- Malicious software (for example, links or pop-up adverts that pose a security

Pupils need to understand that viewing harmful content can have an impact on them. Through our PSHE and Online Safety curriculum they learn:

- Age limits and their purpose.
- Being mindful of what they click on.
- There are different ways harmful content can affect us (for example: violating our rights or the rights of others, affecting our wellbeing and safety, influencing our attitudes or beliefs, influencing our behaviours, be illegal.
- They must speak out to stay safe to a trusted adult.

Use of Artificial Intelligent Software

The use of ChatGPT and other AI-powered software is allowed within the school, under the following conditions:

- Pupils must not use AI tools to impersonate others or engage in deceptive or harmful activities.
- Pupils must not use AI tools to cheat or gain unfair advantages in academic tasks. This includes submitting AI-generated content without proper references or acknowledgment.
- Neither teachers nor pupils should input personal or identifiable data into any AI system without proper guidance or a risk assessment in place.

Pupil Training
As AI technologies continue to evolve, all pupils will receive clear guidance and training on how to effectively, safely, and responsibly use the AI tools they are likely to encounter. This training will be provided through Form Teachers, Tutors and Computing lessons. Pupils will learn about both the technical use and ethical considerations of AI in their academic work and its broader impact on their personal and social lives.

Deepfake Technology

Deepfake technology refers to the use of artificial intelligence to create realistic but false images, videos, or audio recordings of people. These manipulated media can make it appear as though someone is saying or doing something they never actually said or did.

Online Safety and Deepfakes
To keep pupils safe from the misuse of deepfake technology:

- Pupils are taught to recognise that not everything they see or hear online is real or trustworthy.
- Pupils are taught that sharing or creating altered images or videos of others without their permission is wrong and can cause harm.
- Any attempts to use deepfake technology to impersonate, mock, or mislead others, even as a joke, will be considered a serious violation of the school's behaviour policy.
- If a pupil encounters content online that they believe may be fake or manipulated, they should report it to a teacher or trusted adult immediately.

Reporting Concerns
If a pupil or staff member suspects that deepfake content has been shared within the school community, it should be reported immediately to the school's safeguarding team. The school will investigate all incidents and take appropriate action in line with its safeguarding and behaviour policies.

Appendix 3: Technical Security

The school technical systems will be managed in a way to ensure that the school meets the recommended technical requirements

- Responsibility for technical security resides with the Head who delegates this to the Head of IT and information Management
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users are recorded by the Head of IT and information Management and reviewed, at least annually, by the Online Safety Group.
- Security of the username and password must not allow other users to access the systems using their log on details.
- All users have responsibility for the security of their username and password and must not allow other uses to access the systems using their log in detail.
- All school networks and system will be protected by secure passwords.
- The administrator passwords for the school system are keep in a secure place.
- There is a risk-based approach to the allocation of learner usernames and passwords.
- At least, annual reviews and audits of safety and security of learner usernames and passwords.
- Appropriate security measure are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts.
- There are rigorous and verified back-up routines.
- Head of IT and information Management is responsible for ensuring that all software purchased by and used by the school is adequately licenced and the latest software updates are applied.
- Staff are not permitted to install software on a school-owned device without the consent of Head of IT and information Management, which is delegated to the IT Support department.