Online Safety Policy

Draft Prepared	12/09/2020
Date Agreed	*09/12/2020*
Signed by Headteacher	*Teresa Adams*
Signed by Chair of GB	*Rita Hawes*
Date Policy to be Reviewed	1 Year or as required

Overview:

Context

At Goat Lees we recognise our duty to ensure that every child is safe and believe that the same principles to the 'virtual' or 'digital' world that children and young people will encounter as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The purpose of this policy is to:

- Outline the guiding principles for all members of the school community regarding the use of ICT/Computing
- Safeguard and protect the students and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy

This policy applies to all members of school community - staff, students, volunteers, parents and carers, visitors, community users, Governors - who have access to and are users of the school's ICT systems.

Communication of the policy

The policy will be communicated to the school community in the following ways:

- Available on the school website and school policy area
- Included as part of the induction pack for new staff.
- Acceptable use agreements discussed with and signed by students at the start of each year.
- Acceptable use agreements to be issued to whole school community (usually on entry to the school as part of the home school agreement/staff handbook.

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs and vlogs

- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera, video and internet functionality
- Games Consoles (Playstation, Wii, Xbox) with Internet link-up to enable play against players around the world
- PCs, tablets, notebooks and ipads

Although some of these technologies are not available to pupils in school our curriculum is ever changing to ensure that children know how to use these responsibly. This is the world that they are entering when they become adults. All of these are becoming an integral part of their life outside of school and we recognise that the most popular sites change regularly. The exchange of ideas, social interactions and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger. This policy must be read in conjunction with other relevant school policies including (but not limited to): safeguarding and child protection, anti-bullying, behaviour, image use, data, security, GDPR, confidentiality and acceptable use policy, mobile phone and camera, mobile technology and social media.

Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored.

Our online safety officer and DSL ensures they keep up to date with online safety issues and guidance and ensures that the Head, senior management and Governors are updated as necessary.

All staff are responsible for promoting and supporting safe behaviours in their classrooms and around school, following school online safety procedures in line with safeguarding responsibilities. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Key responsibilities *of the school/setting management and leadership team are:*

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of

the school community whilst ensuring children have access to required educational material.

- To work with and support technical staff in monitoring the safety and security of school/setting systems and networks and to ensure that the school/setting network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities
- Ensuring that online safety is embedded within a progressive whole school/setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

Key responsibilities *of the online safeguarding lead/DSLs are:*

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school/setting lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Working with the school/setting leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.

Key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading and adhering to the school/setting Acceptable Use Policies (AUPs)
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong or feel unsure and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networking

- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs and use of website
- Cyberbullying procedures
- Their role in providing online safety education for pupils
- Teaching of online safety on a termly basis

Staff are reminded / updated about online safety matters on a termly basis.

How will complaints regarding online safety be handled?

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Discussion with online safety officer/Headteacher/DSL
- Informing parents or carers
- Referral to LA / Police.

Our online safety officer/DSL acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school Child Protection procedures.

Teaching and Learning

The school has a clear, progressive online safety education programme primarily as part of the Computing curriculum / PSHE curriculum but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The Internet is an essential element in 21st century life for education, business and social interaction. It gives pupils and teachers access to a vast range of online materials, information and experiences that enrich and extend teaching and learning opportunities.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for pupils based on responsible use.

At Goat Lees Primary School we:

- Empower and educate children so they are equipped with the skills to make safe and responsible decisions as well as feeling able to report any concerns.
- Plan pupil's Internet use carefully as part of an integrated curriculum and Computing as a standalone subject. We use a customised online safety school curriclulum using elements of the 'Switched on computing' 'Purple Mash', 'Parent Zone', 'Google Internet Legends' schemes; this allows online safety to be integral in our teaching.
- We use the school's curriculum map to teach online safety in both computing and PSHCE lessons at least termly. We use resources available in school and from the internet. These have been carefully planned for with all parties concerned.
- Teach pupils what Internet use is acceptable and what is not
- Educate pupils in the effective use of the Internet for research, including the skills of knowledge location and retrieval
- Hold regular Key Stage assemblies on using the internet safely and responsibly.
- Teach pupils to be critically aware of materials they access on the Internet and give them guidance on how to validate information before accepting its accuracy.
- Give pupils quick and easy access to 'good' websites through links on the school Intranet and website. Members of staff will always evaluate websites, tool and apps fully before using them with the children.
- Subscribe to online resources such as Spelling Shed and Purple Mash in order to support children's learning within safe online environments.
- Encourage pupils to tell a teacher/responsible adult if they encounter any material that makes them feel uncomfortable.
- Ensure pupils and staff know what to do if they find inappropriate web material (i.e. minimise the tab, turn the device over and report the URL to the teacher – an adult will report this as an online safety concern to DSL)
- Teach online safety as part of the computing and PSHCE schemes of work across the school
- Provide links to good online safety information on our school website
- Ensure that pupils and staff know what to do if a cyber-bullying or other online safety incident occurs, including grooming and extremism.
- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities using the Acceptable Use Agreement signed by every student.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.
- Staff and governor training
- Staff understand the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information.
- Information and guidance on the Safeguarding policy and the school's Acceptable Use Policy is provided to all new staff and governors.

Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

Managing online safety

Goat Lees Primary School has Broadband connectivity provided by the Kent Learning Zone. All computers in the school have Internet access. This provides a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature. Staff and students are aware that they must report any failure of the filtering systems directly to the SLT and technical support.

To maximise the security of the school network and the safety of staff and pupils at Goat Lees we also:

- Keep virus and spyware protection updated regularly
- Never leave pupils unsupervised at a computer
- Block all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Ensure that all staff and pupils are aware of the 'Acceptable Use agreement' before using any school computer to access the Internet.
- The school will consider how to educate pupils in their safe use e.g. use of passwords.
    - ➢ All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
    - ➢ Pupils must not place personal photos on any social network space provided in the school learning platform without permission.
    - ➢ Pupils, parents and staff will be advised on the safe use of social network spaces
    - ➢ Pupils will be advised to use nicknames and avatars when using social networking sites.

General social media use

Expectations regarding safe and responsible use of social media will apply to all members of Goat Lees Primary School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- All members of Goat Lees Primary School community will be encouraged to ▫ engage in social media in a positive, safe and responsible manner at all times.

- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Goat Lees Primary School community.
- All members of Goat Lees Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The use of social networking applications during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of Goat Lees Primary School community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Official use of social media

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- All communication on official school social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official school social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright, GDPR etc.
- Official social media use by the school will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official school social media sites/channels in accordance with the school image use policy.
- Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website.

- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/Carers and pupils will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.
- Primary School has one official social media channel – Facebook.
- Public communications on behalf of the school (school website) will, where possible, be read and agreed by at least one other colleague.
- The school social media account will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and that they are an ambassador for the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on the school social media channel have appropriate parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, and/or the head teacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with pupils or parents/carers through social media and should communicate via school communication channels.

The school also holds a separate Social media policy with further guidance.

Management of applications used to record children's progress.

- The headteacher/manager is ultimately responsible for the security of any data or images held of the chidlren
- Apps/systems which store personal data will be risk assessed prior to use in accordance with GDPR
- Only school/setting issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.

- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the school's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

Managing extremism

The use of social media to engage and incite potential followers is a new phenomenon, changing traditional ideas of how terrorist groups communicate which leads to children and young people being exposed to extremist content in the online world. This threat of exposure to extremism does not just come from groups such as Islamic State, but also from 'far-right' groups. All staff will have taken part in 'prevent' training and complete any additional CPD as required.

At Goat Lees, all staff understand the need for recording any comments that are a cause for concern and seek help through the usual safeguarding procedures. We also aim to educate our children through good quality ongoing online safety and PSHE education. This is essential in helping children and young people develop their own sense of risk and raise their self-esteem and self-worth thus reducing the risk of many forms of harm and abuse, whether radicalisation, sexual abuse, child sexual exploitation, or gang membership, which often start with a grooming process.

Managing Emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Other devices

- Mobile phones and associated cameras will not be used during lessons or formal school time. Only school cameras will be used.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.
- Staff should not share personal telephone numbers with pupils and parents (in exception of school trips where numbers will be discarded in line with GDPR)

Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school/setting address, email and telephone number. Staff or pupils' personal information will not be published.
- The Deputy Headteacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Pupils photos will be published with their permission or that of their parents/carers in line with GDPR

- The administrator account for the school website will be safeguarded with an appropriately strong password.

Using digital Images

Digital images form an important part of our School Environment. Photos of pupils are used for assessment purposes and are displayed on the school website, in books and boards around the school to celebrate pupil's experiences and achievements.
School productions maybe videoed and sold to parents in DVD form, in accordance with photo and video consent.

At Goat Lees Primary we:

- Gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form signed when their child joins the school.
- Never use pupils' names with any photos displayed on the school website or on the display screen in the School reception area.
- Do not include the names of pupils in the credits of any published school produced video materials/DVDs
- Teach pupils to take care what images they choose to display on their own personal social networking sites

Using the school network, equipment and data safely.

The computer network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system and to monitor any Internet or email activity on the network.

At Goat Lees Primary we:

- Ensure that staff read and sign that they have understood the school's online safety Policy. Following this, they are set up with an individual network log-in username and password and an email address
- Provide pupils with an individual network log-in username
- Make it clear that staff must keep their log-in username and password private and must not leave them where others can find
- Make it clear that pupils should never be allowed to log-on or use teacher and staff logins
- Makes it clear that no one should log on as another user
- Have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Require all users to always log off/lock when they have finished working or are leaving the computer unattended
- Ask that when a user finds a computer logged on as someone else they should always log-off and then log-on again as themselves. When away from devices staff are to lock or log off [SIMS times out and requires users to log back in to access]

- Ensure that all pupil level data or any personal data is secure and password protected

Parents and Online Safety

- Parents' attention will be drawn to the School Online Policy and AUP in newsletters, the school brochure and on the school Website.
- Information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home. Some being led by our digital leaders (where applicable).
- All parents will receive support information as and when available.
- Read the Acceptable use policy with their child and encourage them to adhere to it.
- Discuss online safety issues with their own child/ren.
- Role model for their child safe and appropriate use of technology and social media.

Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- All members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils.
- Goat Lees views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads
- The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB "Responding to youth produced sexual imagery" guidance

If the school are made aware of incident involving creating youth produced sexual imagery the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.

- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).

- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- Inform parents/carers about the incident and how it is being managed.
- The school will not view images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school/settings network or devices, then the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- Goat Lees Primary will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- We view online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team by the DSL.

If the school are made aware of incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures

- Immediately notify the designated safeguarding lead
- Store any devices involved securely.
- Immediately inform Kent police via 101 (using 999 if a child is at immediate risk)
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted, then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

Responding to concerns regarding Indecent Images of Children (IIOC)

Goat Lees Primary will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If the school/setting is made aware of Indecent Images of Children (IIOC) then the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.

- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.

If the school are made aware that indecent images of children have been found on the school's electronic devices then the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:

- Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
- Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
- Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.

- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including

anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of Goat Lees community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's online safety ethos.

Sanctions for those involved in online or cyberbullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.

Review and Monitoring

Online safety is integral to other school policies including the Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

The school's online safety coordinator is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and online safety issues in the school.

This policy has been developed in consultation with all other parties involved and approved by the Senior Leadership Team and Board of Governors. Staff will be informed of any updates or amendments to it.

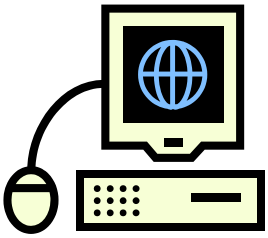
The online safety curriculum can be found in the staff shared area.

General Poster:

Rules for Responsible IT use

We use the School Computers and Internet Connection for Learning. These rules will keep everyone safe and help us to be fair to others.

- I will only log on to computers with my class log on.
- I will keep personal information safe.
- I will not look at other people's files without their permission.
- I will not tamper with or delete other people's files.
- I will not transfer or download files onto school computers without permission (e.g. on a USB drive or from the Internet).
- I will only use the Internet when a teacher has given permission and is present.
- I will not deliberately look for inappropriate websites.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond but I will tell a teacher or another responsible adult.



The School will regularly monitor Internet access to ensure it is being used responsibly.