ONLINE SAFETY POLICY

DATE OF LAST REVIEW :	September 2021
REVIEWED BY :	Governing Body / Executive Head Teacher
DATE OF NEXT REVIEW :	September 2022

Designated Safeguarding Lead (DSL)	Eileen Rogers
Designated Safeguarding Officers	Rebecca Dreesden, Laura Hodgson, Kathryn Dewey, Sarah Copperthwaite, Sian Biggar
Online Safety Lead (if different)	Claire Brayne
Safeguarding Governor	Phil Stickells
PSHE/RSHE lead	Sarah Fox
Network manager / other technical support	Inspired ICT Support or School Business Manager

Contents

AIMS

The school aims to:

- Have robust processes in place to ensure the online safety for all Gorse Ride Schools community members including pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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 cyber-bullying: advice for Head Teachers and school staff
- Relationship Education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

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

ROLES AND KEY RESPONSIBILITIES

This policy applies to all members of the Gorse Ride Schools community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together and support each other in a world that is online and offline at the same time.

EXECUTIVE HEAD TEACHER

The Head Teacher is responsible for ensuring the safety, including online safety, of members of the school community. The Head Teacher will ensure the following:

- Staff with online responsibilities receive suitable and regular training enabling them to carry out their online roles and to train other colleagues as necessary
- There is a clear procedure to be followed in the event of a serious online allegation being made against a member of staff.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- Keep governors and The Senior Leadership Team updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

DESIGNATED SAFEGUARDING LEAD (DSL)

The designated safeguarding lead should take lead responsibility for safeguarding and child protection including online safety. Where the online-safety lead is not the named DSL, ensure there is regular review and open communication between these roles. The DSL's must have overarching responsibility for online safety.

The DSL should be trained in online safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting all staff to understand this policy and that it is being implemented consistently throughout the school
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident (CPOMs)
- Working with the SLT, online safety lead, ICT technician and other staff to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy and the school's safeguarding policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Stay up to date with the latest trends in online safeguarding
- Liaising with other agencies and/or external services if necessary (e.g. technical, pastoral, and support staff as appropriate)
- Providing regular reports on online safety in school to SLT and/or governing board
- Liaise with the local authority [Wokingham] and work with other agencies in line with Working Together to Safeguard Children.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and submit for review to the senior leadership team and governors.
- Embed online safety education across the curriculum and beyond i.e. partnership with parents
- Ensure the 2021 DfE guidance on Sexual Violence and Harassment Between Children in Schools and Colleges is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Ensure appropriate online filtering and monitoring systems are in place to ensure access to illegal content is blocked
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex D of KCSIE (online safety)

GOVERNING BODY

- All governors will ensure that they have read and understood this policy
- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Oversee the school's IT systems and agree and adhere to the terms on acceptable use of the school's ICT systems and the internet – including data and sharing of information

- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Monitor online safety incident logs
- Keep up to date with school online safety matters by having regular reviews with the DSL and incorporate online safety into discussions of safeguarding at governor meetings
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

ALL STAFF

- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and in accordance with school procedures (CPOMs)
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon to the NOLA (formerly LADO)
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum leader, and making the most of unexpected learning opportunities as they arise
- Whenever overseeing the use of technology (devices, the internet etc) in school or setting remote learning, encourage sensible use, monitor what children are doing and consider potential dangers and the age appropriateness of websites and content
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage children to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff
- Be aware of security best-practice at all times, including password hygiene which is the practise of ensure passwords are unique and phishing strategies. Sign and follow the staff acceptable use policy and code of conduct/handbook – including mobile devices

PSHE / RSE LEAD

As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "We want the subjects to put in place the key building blocks of healthy, respectful relationships, focusing on family and friendships, in all contexts, including online" RSE 2001:4). This includes what healthy relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.
- PSHE and RSE will complement the computing curriculum, which covers the principles of online safety at all key stages i.e. how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.

COMPUTING / ONLINE SAFTEY LEAD

As listed in the 'all staff' section, plus:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the National Curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements
- Work with the wider school community (i.e. parents) to promote online safety
- Look for opportunities to embed online safety in your subject and model positive attitudes and approaches to staff and pupils alike
- Report to the governors and meet them as required
- Liaise with local authority
- Provide resources and websites to enhance the Computing curriculum
- Ensure subject specific action plans also have an online-safety element

ICT TECHNICIAN

The external ICT Technician and, where appropriate, the Online Safety Lead, DPO and DSLs will be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s), ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve ensuring the following:

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that school systems and networks reflect school policy

- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL, OSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Log and report any online safety incidents in line with school policy
- Appropriate safeguards are in place for Remote Learning – see remote learning policy

DATA PROTECTION OFFICER (DPO) – SCHOOL BUSINESS MANAGER

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document: "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."
- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area.
- Work with the DSL and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- Work with the Head Teacher to ensure the school website meets statutory DfE requirements

PARENTS

Parents are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 3)

REVIEWING, REPORTING AND SANCTIONS

Review

- This policy will be reviewed and updated annually, or sooner if necessary
- The school will review the effective implementation of the online policy

Acceptable Use Agreements

- All users of the school computers including all staff and pupils will read and follow the appropriate Acceptable Use Agreement (See Appendix 1-5).
- The Acceptable Use Agreements will be shared with parents to help support for the school's policy.

Reporting

- Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour, safeguarding and ICT acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.
- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- All pupils and teachers should be aware of these guidelines.

Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour, rewards and sanctions.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

EDUCATING CHILDREN ABOUT ONLINE SAFETY

Children will be taught about online safety as part of the curriculum
The text below is taken from the National Curriculum computing programmes of study.
It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- **The EYFS framework** sets the standards to make sure that children aged from birth to 5 learn and develop well and are kept healthy and safe. Online safety must be incorporated into the curriculum in the early years

In **Key Stage 1**, 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 2** will be taught to:

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

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

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

Educating Parents

- Read and promote the school's parental acceptable use policy (AUP), Including remote learning policies and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Sharing resources and information via newsletters, email, and website where appropriate
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, Proprietor, contractors, pupils or other parents/carers

COMMUNICATIONS & COMMUNICATIONS TECHNOLOGIES

Mobile phones and personal handheld devices

Pupils

- Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school. Mobile phones are kept in the office during the school day.
- The sending of abusive or inappropriate text messages or images will be viewed as serious and fully investigated.
- If necessary, searches will be made for mobile phones/technology if staff have become aware that children may have them in school (and have not put them in the office) or have them during an off-site visit e.g. school residential. Phones will be confiscated if this is the case and returned at an appropriate time to the child or parent.
- Pupils will not be allowed to bring in games devices and other electronic equipment, particularly those which allow ad hoc networks to be established.

Staff Members (including volunteers, professionals, contractors and students on placement) may bring mobile phones onto the school site on the understanding that:

- Mobile phones are not permitted in areas where children are present
- Only used during break times and at either end of the school day (when children are not present)
- Employees are not permitted to make/receive calls/texts during lessons or formal school time and staff use of mobile phones during the school day will normally be limited to the morning/lunch break and after school
- Mobile phones should be switched off (or silent) and left in a safe place during lesson times
- Staff should only use phones in designated areas; the staff room or office spaces
- When off-site, designated members of the group will have a mobile phone available for emergency contact with the school, with each other or with the emergency services. In this context phones will not be used to make or receive personal calls
- Personal mobile phones must not, under any circumstances, be used to take images or videos of children. If images or videos, are required for educational purposes, they must be taken using a school device and images securely stored on the school's network
- Teacher/parent contact should be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone or SLT permission has been sought. Teachers should always withhold their number and delete any parent numbers contacted

The above information is shared with new staff members as part of the induction process.

Visitors (including parents)

- Model safe, responsible and professional behaviours in their own use of technology
- Mobile phones are not permitted in areas where children are present
- Visitors may only use their phones if needed in either the school office or staffroom
- Report any concerns, no matter how small, to the designated safeguarding lead
- It is the responsibility of all staff members to exercise vigilance at all times and to raise concerns as soon as possible, either directly with the person who is contravening expectations or by reporting the incident to a senior leader as soon as possible after the event.

E-mail and messaging

- Staff will be informed that the use of school e-mail accounts will be monitored.
- Staff must not use personal web-based e-mail accounts, or other social media apps, to communications with parents or pupils.
- Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.
- Pupils wishing to send e-mails to an external person or organisation must be authorised by a member of staff and sent via a teacher's email account.

Social networking

- For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction.
- Staff have a right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity. Staff MUST NOT use personal social networking sites to contact parents or pupils.
- Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.
- Social media has been identified as an important tool in the sharing of extreme material and extremist groups are actively using social media to inform, share propaganda, radicalise and recruit for their cause. Social media safeguarding is an important element of protecting young people from extremist narratives. "PREVENT" can play an active part in the process.
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

To report any online terrorist related material go to www.gov.uk/report-terrorism

Internet usage

- Pupils and staff will be informed that internet access will be monitored.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Users must not attempt to disable or reconfigure any filtering, virus protection or similar.
- Pupils will receive guidance in responsible and safe use on a regular basis
- All pupils, parents, staff, and governors are expected to read and follow an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-4).
- Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
- We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

At this school, the internet connection is provided by RM until Feb 2022, Inspired ICT and Schools Broadband from Feb 2022 onwards. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called RM SafetyNet (until Feb 2022) FortiGate and NetSweeper (from Feb2022), which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At Gorse Ride Schools we have decided that option 1 and 2 are appropriate because It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Digital and video images

Parents, staff and pupils may record images of pupils at school under the following conditions:

- Parental permission must be obtained for the taking and use of digital and video images of pupils.
- Images should not be used on school learning platforms and/or websites or publicity without express permission from the parent, and where such permission has been obtained individual pupils should not be identifiable by name.
- All staff digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny by managers if required.
- The use of staff personal devices is not acceptable unless agreed with a member of SLT in advance and for a specific purpose.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Images should not be distributed beyond either the school or the immediate family and friends of the pupil’s family.
- Images of pupils must be stored securely and deleted when no longer required.
- No images of pupils should be recorded in toilets or wash areas, whilst pupils are getting changed or in the medical room. The only exceptions to this rule would be if images are recorded to illustrate a particular point for display (e.g. how to wash hands). In this case the line manager must be informed before this activity is undertaken.

Home Learning

The school has the capability to use TEAMs video conferencing technology to allow all pupils to access learning from home and communicate with their teacher if necessary e.g. during lockdown. The school has created a specific set of guidelines to manage such an events. Parents must have read the Acceptable User Guidelines.

See Remote Learning policy

CYBER-BULLYING

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.
- We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. [Class teachers] will discuss cyber-bullying with their class.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.
- Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Break any of the school rules

If inappropriate material is found on the device, the staff member must consult with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- *The school's COVID-19 risk assessment*

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

LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- *Child protection and safeguarding policy*
- *Behaviour policy*
- *Staff Code of Conduct*
- *Data protection policy and privacy notices*
- *Complaints procedure*
- *ICT and internet acceptable use policy*

MONITORING ARRANGEMENTS

- The DSL reviews behaviour and safeguarding issues related to online safety on CPOMs
- This policy will be reviewed every year by the [Head Teacher and Computing Lead]. At every review, the policy will be shared with the governing board.

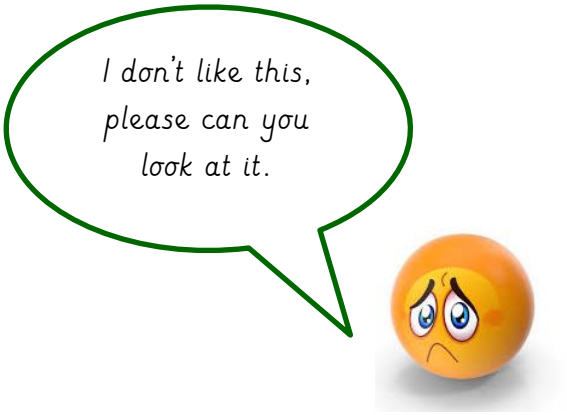
APPENDIX 1: ACCEPTABLE USE AGREEMENT – INFANT PUPILS

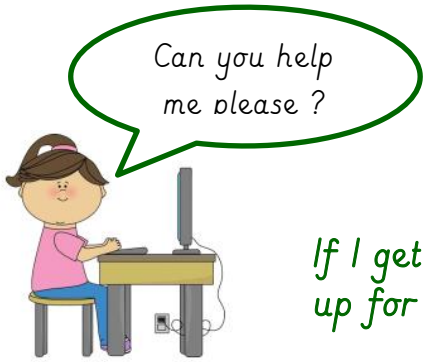
ACCEPTABLE USE AGREEMENT - PUPILS

This document is intended for all KS1 pupils (Reception, Year 1 and Year 2) and their parents/carers.

KS1 E-Safety Agreement – keeping me safe at home and at school

If I see something or read something that makes me feel worried or unhappy or upset, I will tell a grown up straight away





If I get stuck or lost on the internet I will ask a grown up for help

I will always send polite and friendly messages

I will only send messages to people I know

I will keep my personal information (my name, my address, my school) secret and not share it online

APPENDIX 2: E-Safety Agreement - Pupil Declaration

Parent/Carer support for Pupil Acceptable Use Agreement

As the parent/carer of the above pupil, I confirm that I, with my child, have read and discussed Gorse Ride Schools Acceptable Use Agreement.

I am confident that my son/daughter has understood the importance of online safety and this agreement.

I understand that my son/daughter will have access to the internet and to IT systems at school. I am aware that this activity will be monitored for safety and security reasons to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection and human rights legislation.

I know that my child has received, or will receive, online safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that although internet filtering systems usually work very well, inappropriate content may occasionally still be accessible, but in this instance the school will take appropriate action with the service provider to request such content is removed.

I fully support the school's online safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

I will inform the school if I have any concerns over my child's, or any other members of the school community's online safety.

I know that I can visit the following websites for further information about keeping my child safe online.

- www.thinkuknow.co.uk/parents
- www.internetmatters.org
- www.saferinternet.org.uk
- www.childnet.com

Child's Name:		Class :	
Parent Signature:		Date:	

Appendix 3: ACCEPTABLE USE AGREEMENT – JUNIOR PUPILS

This document is intended for all KS2 pupils (Years 3 – 6) and their parents/carers.

KS2 E-Safety Agreement

For my own personal safety:

- I will ask permission from a member of staff before using the Internet at school.
- I will only use the Internet when a responsible adult is in the room.
- I am aware of 'stranger danger' when online and will not meet online friends in real life.
- I will not tell anyone my username or password nor will I try to use any other person's username and password.
- I will not give out any personal information (e.g. full name, home address, telephone number, birthday, school) about myself or anyone else when online that could be used to identify me, my family or my friends unless a trusted adult has given permission.
- I will not arrange to meet people offline that I have communicated with online.
- I will be very careful when sharing pictures or videos of myself or my friends and if I am at school I will always check with a teacher first. I know that once a picture has been shared it cannot be deleted – however silly or embarrassing it is.
- I will only play video games that are suitable for my age.
- I am aware that some websites and social networking sites have age restrictions and I should respect these.
- If I receive a message that upsets me or makes me feel uncomfortable, I will not respond to it or delete it and I will immediately show it to a teacher or responsible adult so it can be traced back to the sender.
- I will immediately report any unpleasant or inappropriate material or anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school IT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not use the school IT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

Acting as I expect others to act toward me:

- The messages I send will be polite and responsible.
- I will respect others' work and property and will not access, copy, remove or otherwise alter anyone else's files, without the person's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I respect that others may have different opinions.
- I will not take or share images of anyone without their knowledge and permission.

Keeping secure and safe when using technology in school:

- I will only use approved e-mail or message accounts on the school system.
- I will not use my personal handheld/external devices (e.g. mobile phones, USB devices, etc.) in school.
- I will only use the school's computers for schoolwork and homework.
- I will not try to upload, download or access any materials or files which are illegal or inappropriate or may cause harm or distress to others or which may be harmful to the school's IT systems
- I will immediately report any damage or faults involving equipment or software.
- I will not open any attachments to e-mails, unless given permission to do so and I know and trust the person/organisation that sent the e-mail.

- I will ask for permission before sending an e-mail to an external person/organisation
- I will not try to bypass the system to reach websites or apps that the school has blocked
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will immediately tell a staff member if I receive an offensive e-mail or message.
- I understand that the school will monitor my use of the IT systems, e-mail and other digital communications when at school.

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I understand that the school may take action against me if I am involved in incidents of inappropriate behaviour whether this is inside or outside of school. If the activities are illegal, this may be reported to the police.
- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

APPENDIX 4: ACCEPTABLE USE AGREEMENT – STAFF

This document is intended for all staff, temporary workers, volunteers and other parties who may have access to the schools' information systems.

Purpose

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's Online Safety policy for further information and clarification.

Declaration

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Executive Head Teacher.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware (eg on a school laptop / device) unless authorised.
- I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school Online Safety policy and Data Protection policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that pupil use of the internet is consistent with the school's Online Safety Policy.
- When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. Online Safety Co-ordinator, Designated Safeguarding Lead and/or SLT member.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Signed : _____

Print Name : _____

Position : _____

Date : _____