Gorse Hall Primary and Nursery school

Online Safety Policy

Last reviewed: November 2021

Review date: November 2022

Contents:

Statement of intent

"Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks.

We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world."

*'**Teaching** online safety in school' DFE non-statuary guidance June 2019 – Not been updated on DFE website since 2019*

Protecting young people and adults properly means thinking beyond the school environment. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Gorse Hall pupils will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

The breadth of issues classified within online safety is considerable, but they can be categorised into four key areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and /or financial scam.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Online safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.

- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behavior and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behavior is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimize the risk of misplaced or malicious allegations made against adults who work with pupil.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2021) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'This policy operates in conjunction with the following:
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Behavioural Policy
- Disciplinary Policy and Procedures
- GDPR Policy
- Photography Policy
- Acceptable Use Agreement
- Staff Code of Conduct

Signed by:

Headteacher Date: November 2021

Chair of Governing Board Date: November 2021

1.Teaching and Learning

Why the internet and digital communications are important

1.1. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

1.2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

1.4. Staff model safe and responsible behavior in their use of technology during lessons.

Internet use will enhance learning

1.5. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

1.6. Pupils will be taught what internet use is acceptable and what is not.

1.7. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

1.8. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

1.9. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

1.10. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

1.11. Pupils will be taught how to report unpleasant internet content to class teacher. This can be done anonymously, or in person, and will be treated in confidence.

1.12. The school has a clear, progressive online safety education programme as part of the computing/PSHE/HSE/RSE curriculum. This covers a range of skills and behaviors appropriate to their age and experience, including:

- To understand what they may be consenting online to
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.

- To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behavior when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behavior; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files – without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, peer on peer abuse, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

2. Managing internet access

Information system security

2.1. School ICT systems security will be reviewed regularly.

2.2. Virus protection will be updated regularly.

2.3. Security strategies will be discussed with the LA.

Email

2.4. Pupils may only use approved email accounts on the school system.

2.5. Pupils must immediately tell a teacher if they receive an offensive email.

2.6. In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.

2.7. Incoming emails will be treated as suspicious and attachments not opened unless the author is known.

2.8. The school will consider how emails from pupils to external bodies are presented and controlled.

2.9. The forwarding of chain letters is not permitted.

2.10. The school:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.
- Will contact the police if one of our staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make emails dangerous.

Published content and the school website

2.11. Staff or pupil personal contact information will not be published.

2.12. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.

2.13. Uploading of information is restricted to our website authorisers.

2.14. The school website complies with the following statutory DfE guidelines for publications:

- What maintained schools must publish online

2.15. Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

2.16. The point of contact on the website is the school address and telephone number. The school uses a general email contact address: admin@gorsehall.tameside.sch.uk. Home information or individual email identities will not be published.

2.17. Photographs published on the web do not have full names attached.

2.18. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Publishing pupils' images and work

2.19. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.

2.20. Written permission from parents will be obtained before photographs of pupils are published on the school website. .

2.21. Pupil image file names will not refer to the pupil by name.

2.22. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.23. The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form completed annually.

2.24. The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

2.25. Staff sign the school's Acceptable Use Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.

2.26. If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, the school will obtain individual parental or pupil permission for their long-term use.

2.27. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.

2.28. Pupils are taught about how images can be manipulated in their online safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

2.29. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

2.30. Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

2.31. This policy should be read in line with our Photography policy.

Social networking and personal publishing

2.32. The school will control access to social networking sites and consider how to educate pupils in their safe use.

2.33. Newsgroups will be blocked unless a specific use is approved.

2.34. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

2.35. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

2.36. Pupils will be advised to use nicknames and avatars when using social networking sites.

2.37. Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.

2.38. Staff will be shown how to 'block' their profile picture from being downloaded and protect their profile information.

2.39. Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites. Staff will be encouraged not to tag co-workers into photographs that may show them in a negative light.

2.40. Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the school's preferred system for such communications.

2.41. School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Managing filtering

2.42. If staff or pupils come across unsuitable online materials, the site must be reported to the online safety coordinator.

2.43. Senior staff and the ICT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing and webcam use

2.44. Videoconferencing should use the educational broadband network to ensure quality of service and security.

2.45. Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

2.46. Videoconferencing and webcam use will be appropriately supervised.

Managing emerging technologies

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

2.48. The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

2.49. Mobile phones will not be used during lesson time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

2.50. The use by pupils of cameras in mobile phones will be kept under review.

2.51. Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

Protecting personal data

2.52. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

Personal devices and mobile phones

2.53. The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded.

2.54. The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.

2.55. Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

2.56. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

2.57. The Bluetooth, or similar function, of a mobile phone will be switched off at all times and not be used to send images or files to other mobile phones.

2.58. No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

2.59. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity unless agreed by the headteacher.

2.60. Staff will use the school phone where contact with pupils' parents is required unless agreed by the headteacher.

2.61. If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, it will only take place when approved by the SLT.

2.62. Staff will not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.

2.63. If a member of staff breaches the school policy, disciplinary action may be taken.

2.64. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, permission will be sought by the headteacher.

2.65. Pupils will abide by the following rules when using personal devices in school:

- The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. Pupils must sign their mobile phone in and out and it will be kept locked in the school office until the end of the school day.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents in accordance with the school policy.
- If a pupil needs to contact their parents, they will be allowed to use a school phone. Parents are advised not to contact their child via

their mobile phone during the school day, but to contact the school office.

- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

3. Roles and responsibilities

3.1. The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety).

· Ensuring that there are appropriate filtering and monitoring systems in place.

3.2. The **headteacher** is responsible for:

- Supporting the DSL, any deputies and subject Leads by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing board to update this policy on an annual basis.

3.3. The **DSL** is responsible for:

- Taking the lead responsibility for online safety in the school alongside the Computing Subject Leads.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

- Liaising with relevant members of staff on online safety matters, e.g. the subject leads, SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher, subject leads and governing board to update this policy on an annual basis.

3.4. **ICT** technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.

3.5. All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

3.6. Pupils are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

4. Policy decisions

Authorising internet access

4.1. All staff will read and sign the Acceptable Use Agreement before using any school ICT resource.

4.2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

4.3. At EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

4.4. Any person not directly employed by the school will be asked to sign the Acceptable Use Agreement before being allowed to access the internet from the school site.

Assessing risks

4.5. The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access.

4.6. The school should audit ICT use to establish if the Online safety Policy is adequate and that the implementation of the Online safety Policy is appropriate and effective.

Handling online safety complaints

4.7. Complaints of internet misuse will be dealt with by a senior member of staff.

4.8. Any complaint about staff misuse must be referred to the headteacher.

4.9. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

4.10. Pupils and parents will be informed of the complaints procedure.

4.11. Pupils and parents will be informed of the consequences for pupils misusing the internet.

Community use of the internet

4.12. The school will liaise with local organisations to establish a common approach to online safety, if necessary.

5. Pupil online safety curriculum

Teaching and learning

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

5.1. This school has a clear, progressive online safety education programme as part of the computing/PSHE/RSE/Citizenship curriculum. This covers a range of skills and behaviors appropriate to the age of the children, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To know how to narrow down or refine a search.
- To understand acceptable behavior when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behavior; keeping personal information private.

- To understand why online ‘friends’ may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

5.2. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

5.3. The school will remind pupils about their responsibilities through a Pupil Acceptable Use Agreement which every pupil will sign.

5.4. All staff will model safe and responsible behavior in their own use of technology during lessons.

Online risks

5.5. The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

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 classes.

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.

5.6. Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." – BullyingUK.

5.7. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy/Safeguarding and Child protection policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

5.8. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

5.9. Posters providing information about how to get help from Childline, ThinkUKnow and the NSPCC are displayed on the children's information board in the main corridor and at other highly visible points.

5.10. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated.

5.11. There are clear procedures in place to support anyone in the school community affected by cyber bullying.

5.12. All incidents of cyber bullying reported to the school will be recorded.

Sexual exploitation/sexting

5.13. Sexting between pupils will be managed through our anti-bullying procedures.

5.14. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.

5.15. There are clear procedures in place to support anyone in the school community affected by sexting.

5.16. All incidents of sexting reported to the school will be recorded.

Radicalisation or extremism

5.17. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

5.18. Extremism is defined by the Crown Prosecution Service as "The demonstration of unacceptable behaviour by using any means or medium to express views which:

- Encourage, justify or glorify terrorist violence in furtherance of beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
- Foster hatred which might lead to inter-community violence in the UK."

5.19. The school understands that here is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

5.20. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.

5.21. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

5.22. The school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

5.23. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

6. Communications policy

Introducing the Online safety Policy to pupils

6.1. Online safety rules and guidance posers will be displayed in corridors and communal spaces and discussed with pupils regularly. An online safety display will be kept up-to-date in the library.

6.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

6.3. A programme of training in online safety will be developed by the computing coordinator, PSHE coordinator, RSE coordinator and DSL.

6.4. Safety training will be embedded within the computing, RSE and PSHE schemes of work in line with national curriculum expectations.

Staff and the online safety policy

6.5. All staff will be given the school Online safety Policy and have its importance explained.

6.6. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

6.7. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

6.8. Staff will always use a child friendly safe search engine when accessing the web with pupils. Staff will be vigilant so that pupils do not use a child friendly safe search engine.

Remote learning

6.1 All remote learning is delivered in line with the school's Pupil Remote Learning Plan.

6.2 All staff and pupils using video communication must:

- Communicate in groups.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

6.3 All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.

- Always remain aware that they can be heard.

6.4. The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.

6.5 Pupils not using devices or software as intended will be disciplined in line with the Behavioural Policy.

6.6 The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

6.7 The school will consult with parents at least two weeks prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

6.8. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

6.9. The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

7.0 During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

17.1 The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Enlisting parents' support

- Parents' attention will be drawn to the school Online safety Policy in an online safety leaflet, newsletters, and the school brochure and on the school website.
- The school will maintain a list of online safety resources for parents.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

- The school will have a page on its website dedicated to keeping children safe online. It will provide parents with useful links to help them in understanding the internet.

Online safety Activities and Issues

Activities	Key online safety issues
Creating web directories to provide easy access to suitable websites	• Parental consent should be sought • Pupils should be supervised • Pupils should be directed to specific, approved online materials
Using search engines to access information from a range of websites	• Filtering must be active and checked frequently • Parental consent should be sought • Pupils should be supervised • Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with
Exchanging information with other pupils and asking questions of experts via email or blogs	• Pupils should only use approved email accounts or blogs • Pupils should never give out personal information
Publishing pupils' work on school and other websites	• Pupil and parental consent should be sought prior to publication • Pupils' full names and other personal information should be omitted • Pupils' work should only be published on moderated sites and only by the ICT technician.
Publishing images, including photographs of pupils	• Parental consent for publication of photographs should be sought • Photographs should not enable individual pupils to be identified • File names should not refer to the pupil by name • Staff must ensure that published images do not breach copyright laws
Communicating ideas within chat rooms or online forums	• Only chat rooms dedicated to educational use and that are moderated should be used • Access to other social networking sites should be blocked • Pupils should never give out personal information
Audio and video conferencing to gather information and share pupils' work	• Pupils should be supervised • The school should only use applications that are managed by LAs and approved educational suppliers
Social networking	• Staff should set their profiles to private and ensure they do not accept friend requests from pupils or parents • Social networking sites should be blocked on the school network • Pupils should be educated in the dangers involved in 'friending' or talking to people they do not know online

Useful Resources for Teachers and Parents

Resource	Website
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Family Online Safety Institute	http://www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Internet Safety Zone	www.internetsafetyzone.com
Vodafone digital parenting	www.vodafone.com/content/digital-parenting.html
NSPCC - Share Aware	www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone	www.theparentzone.co.uk/school
Teaching Online Safety Guidance	www.gov.uk
Education for a Connected World Framework	www.gov.uk

Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher.

- I will only use the school's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or governing board.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the headteacher or governing board and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the headteacher.
- I will report any accidental access to inappropriate materials immediately to my line manager.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or headteacher in line with data security policy.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the headteacher.

- I will respect copyright and intellectual property rights.

    - I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).

    - I will support and promote the school's Online safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature ______________________________

Date ______________________________

Full name ______________________________ (Printed)

Gorse Hall School
STALYBRIDGE

Acceptable Use Agreement: Pupils

Class: ______________________

Year: _______________________

Pupil Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- I will only use my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords for the learning platform, school network or for other learning websites.
- I will only open/delete my own files.
- I will make sure that all ICT related contact with other children and adults is appropriate and polite.
- I will not deliberately look for, save or send anything that could offend others.
- If I accidentally find anything inappropriate on the internet I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number, home address or school.
- I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I know that my use of ICT can be checked and that my parent contacted if a member of school staff is concerned about my safety.
- I will not bring a mobile phone or other personal ICT device into school.

Signature pupil: ________________________

Signature parent: ________________________

Date: ____________________

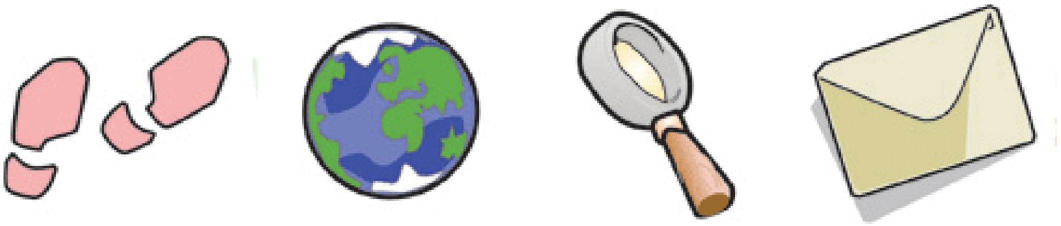
Rules for EYFS and KS1

Think then Click

These rules help us to stay safe on the internet

Online safety rules for EYFS and KS1

- ✓ We only use the internet when an adult is with us.
- ✓ We can click on the buttons or links when we know what they do or where they take us.
- ✓ We can use the internet to search for things when an adult is with us.
- ✓ We always stop and ask for help if we get lost on the internet.
- ✓ We can send and open emails with a grown-up.
- ✓ We can write polite and friendly emails to people we know.
- ✓ We never share our names or addresses on the internet.
- ✓ We know that friends are people we know in the real world not people we meet online.



Gorse Hall School
STALYBRIDGE

Rules for KS2

Think then Click

These rules help us to stay safe on the internet

Online safety rules for KS2

- ✓ We ask permission before using the internet.
- ✓ We only look at websites an adult has given us permission to use.
- ✓ We always tell an adult if we have seen, heard or read anything on the internet that has made us feel threatened, uncomfortable or worried.
- ✓ We immediately close a web page if we are unsure.
- ✓ We only send polite and friendly emails to people we know or that an adult has approved.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don't know.
- ✓ We do not open emails sent by anyone we don't know.
- ✓ We do not use internet chat rooms.
- ✓ We know that friends are people we know in the real world not people we meet online.