Garswood Primary School Policy for Online safety

In conjunction with 'GIST'

(Garswood Internet Support Team)

"Harnessing Technology: Transforming learning and children's services sets out the government plans for taking a strategic approach to the future development of ICT."

http://www.dfes.gov.uk/publications/e-strategy/

The policy has been created by a working party consisting of computing lead, SLT and head teacher, GIST (Garswood Internet support team (made up of KS2 children) and then discussed and approved by Parents, Staff and Governors.

Last updated: June 2023

GIST (Garswood Internet Support Team)

What is Garswood's Internet Support Team

Garswood's Internet Support Team is a network of children across KS2 who show an aptitude towards computing and a particular interest in e safety across the school. Meeting are led by Miss Moon the computing lead and discussions from team meetings are shared with the deputy head and specific learning assistants. They are involved in all major e safety decisions across the school and will often disseminate information across the school.

What does the team do?

The GIST Team created an action plan to ensure e safety is current and happening across Garswood Primary, training is in place and policies are adhered to. They create, plan and deliver training across the school and share results and information they have gained with staff and Governors.

How do they tackle e safety at Garswood?

The team have a number of duties with regards to e safety, their action plan includes....

- Creating presentations to staff and pupils
- Carry out surveys and analyse the information gained.
- Create posters and information leaflets for various audiences with regards to e safety.
- Discuss policies and action plans and ways to move forward
- Create online and virtual resources for various people to access.
- Create solutions to e safety problems as they arise.

This e-safety policy was approved by the Governing Body / Governors Sub Committee on:	
The implementation of this e-safety policy will be monitored by the:	Computing lead – Les Moon, GIST, SLT
Monitoring will take place at regular intervals:	Annually (October)
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2024
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Computing lead – Les Moon, Family Support Worker – H Evans Head teacher – Pam Potter

Education for a Connected World:

Today's children and young people are growing up in a digital world. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online.
Garswood will adopt philosophies from Education for a Connected World to describe the skills and understanding that children and young people should have the opportunity to develop at different ages and stages. Highlighting what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it safely.

ProjectEVOLVE:

Resources each of the 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World" with perspectives; research; activities; outcomes; supporting resources and professional development materials.
This vast library of content is managed by an innovative new engine, designed by the SWGfL Webteam, that not only makes navigating the content intuitive but allows users to personalise the content they collate.
Project evolve can provide information, lesson plans, research summaries, stimulus questions and activities for pupils to complete. Professional development materials for staff are also available to broaden ever changing e safety knowledge. It has been designed with customisation and flexibility.
The content has been written by a team of experts here at the UK Safer Internet Centre. It's up to date; relevant and engaging and moves online life education into the third decade of the 21st century.

Aims:

Garswood will use Project Evolve, Google Legends and Education for a Connected World as a tool for anyone who works with children and young people. It enables the development of teaching and learning as well as guidance to support children and young people to live knowledgeably, responsibly and safely in a digital world.

They focus specifically on eight different aspects of online education:

1. Self-image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

Garswood and Education for a Connected World aims to support and broaden the provision of online safety education, so that it is empowering, builds resilience and effects positive culture change. The objectives promote the development of safe and appropriate long-term behaviours, and support educators in shaping the culture within their setting and beyond.

In conjunction with various advisors Garswood is developing a rich, effective and developmental curriculum, which will support young people to be safe, healthy and thriving online:

- Auditing and evaluating existing provision of online safety education
- Coordinating delivery of online safety education throughout the curriculum
- Improving engagement across the wider school community on issues related to online safety
- Developing effective training for staff and governors/board members

Online safety is a whole school issue. The framework aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed, however, to be usable across the curriculum and to be central to a whole school approach to safeguarding and online safety.

Overview:

This e safety policy applies to all members of Garswood Primary (including staff, pupils, volunteers, parents, trainee teachers, visitors) who have access to and are users of Garswood Primary both in and out of the *school.*

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and devices as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

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

- The Internet and e-mail
- Instant messaging often using web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms Gaming Sites
- Music download sites Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Roles and Responsibilities:

Our e-Safety Policy has been written by the school, building on the information from **Education for a Connected World, Becta, CEOP and GIST team discussions.**

The school's e-safety policy will operate in conjunction with other policies including those for Computing, behaviour, Cyber bullying and Child Protection.

The **e safety coordinator (Les Moon)** will operate as part of the Computing coordinators role in association with the **SENCO (Lucy Myatt)** and **Pastoral Lead (Helen Evans)** all discussions and specific incidents on violation of e safety will be recorded on CPOMS flagged to the **deputy head and head teacher (Andrew Yearsley and Pam Potter)**

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer/Safeguarding Unit and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors – Governors / Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. They will regularly receive internet filtering and monitoring reports and one specific member will take the role of e-safety officer in the Governing Body.

Head teacher - The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator. The Headteacher and computing lead (SLT member) are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Online safety coordinator –

- leads the e-safety team (GIST)
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority and liaises with school technical staff
- receives reports of e-safety incidents and uses these to inform future e-safety developments,
- meets regularly with SLT to discuss current issues, review incident logs and filtering / change control logs
- attends relevant governors meetings

St. Helens technicians:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the internet filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

Teaching and Support Staff:

- they have an up to date awareness of e-safety matters at Garswood and its e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher / family support worker or E-Safety Coordinator
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

GIST (Garswood Internet Safety Team):

The GIST provides a consultative group that has representation from KS2 children and staff with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the GIST will assist the e safety coordinator, Miss Moon with:

- the production / review / monitoring of the school e-safety policy.
- the production / review / monitoring of the school e safety action plan.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression.
- consulting parents / carers and pupils about the e-safety provision.
- monitoring improvement actions identified through use of questionnaires and surveys.

E Safety:

E safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

• Key e-safety messages should be reinforced as part of a planned programme of assemblies and lessons.

• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

• Staff should act as good role models in their use of digital technologies the internet and mobile devices

• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

• Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education/Teaching and Learning

Why Internet use is important

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

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. It operates closely with Garwood's creative curriculum, encouraging children to do their own research both in and outside of school connected with their own learning.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to St Helens firewall requirements outlined below:

2.1. *Filtered access to the Internet in schools is provided to members of staff in pursuance of their duties in schools. Access should only be attempted by members of staff who have been authorised to do so by the Head Teacher.*
2.2. *Members of staff using the internet in schools must do so within the general requirements of the School's Code of Conduct, with particular regard to*

- **Duty of Fidelity -** *includes actions or omissions which could damage the business prospects or reputation of the school or in any way bring the school into disrepute.*
- **Duty of Care -** *is defined as carrying out your particular occupation using the skills, ability and knowledge for which you are employed to the best interest of the Council/School and using Council/School equipment and resources with proper regard.*
- **Use of Council/School Property or Facilities -** *you must not remove or use School property for your personal requirements or for the benefit of others where the work of the School is not involved. Use of School buildings or facilities outside your normal duties and hours of work must be fully authorised and open to scrutiny.'*

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

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

Pupils will be taught how to evaluate Internet content

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

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
Current Garswood software such as **smoothwall** will filter inappropriate images before children become aware of them but the searching of images will be taught through whole class lessons.

Parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's / academy's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community
- Supporting community groups eg Tots Club

Training:

Staff:

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

• A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.

• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.

• The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

Governors:

Governors should take part in e-safety training with particular importance for those who are assigned to e safety and child protection.

• Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be updated daily through **Smoothwall** downloading automatically through the schools networked server. Image protection to avoid inappropriate viewing of flesh tone will be highlighted, record and blocked by the **Smoothwall** software brought into Garswood to cover the areas that **Smoothwall** is not equipped to prevent.

Microsoft Teams and E mail accounts:

Pupils may only use approved e-mail accounts on the school system. Each Year group have been allocated a username and password to Microsoft Teams which operates without their our 'class' with one username and password to be used during lesson time to demonstrate and develop curriculum objectives, and for Home learning. Aany use of 'messaging' will take place through Teams to specific members of their own class or allocated staff, were all messages sent can be edited and accounted for. No messages will be sent externally to anyone who does not attend Garswood Primary School. When blogging on the school website or Teams children must always access their account. Pupils must immediately tell a teacher immediately if they receive offensive e-mail or messages. Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission. *(Refer to e bullying policy and safer Internet Day resources on staff share)*

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

ST Helens services advice....

Head Teachers should critically consider the granting of Internet access to ensure that usage will add value to the member of staff's role in the school. Head Teachers should also ensure that all members of staff are aware of the need for this authorisation before attempting to use the Internet and that any unapproved connection may constitute a breach of the Code of Conduct.

Head Teachers should immediately request the removal of Internet access for leavers and for any member of staff suspended from work. This information should also be made available to St. Helens.

Published content on the School Spider Website

The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Computing co-ordinator and website lead will take overall editorial responsibility and ensure that content is accurate and appropriate.

The School spider website will be updated regularly with current school information such as newsletters, home activities, class topic information and dates throughout the term. The class teacher and office manager will be responsible for this.

Only children who have signed and written permission from their parent or Guardian will have photographs, school work, birthdays and full names uploaded.

Publishing pupil's images on Teams, Garswood Website and Twitter

Only children with written permission from a Parent or Guardian will have photographs and class work published on the website or Twitter.

Pupils' full names will not be displayed as part of the uploaded work, but first names could be associated with individual photographs or pieces of work

Written permission from parents or Guardians will always be sought when a new child starts at Garswood School

Pupil's work can only be published with the permission of the pupil as well as the written permission mentioned above.

Social networking and personal publishing

The school will block/filter access to social networking sites through the St Helens filtering system. Twitter will only be allowed with head teachers permission.

Free Online games, especially those containing aspects of violence will be blocked and reported immediately to St Helens in order for the particular URL to be added to the LA's blocked list.

Pupils will be advised **never** to give out personal details of any kind which may identify them or their location. *(Refer to e bullying policy and safer Internet Day resources on staff share)*

Pupils and parents will be advised that the use of social network spaces outside school is mostly inappropriate for primary aged pupils.

Managing filtering

In conjunction with the St. Helens LA Internet policy, has adopted the following actions:

3.2. *Internet access is provided to schools through the St Helens MAN (Metropolitan Area Network). This infrastructure provides an Internet firewall and a filtering mechanism, presently installed at either school or LEA level. Members of staff should not attempt to circumvent or disable any of these features.*

3.3. *Members of staff should use their individual I.D. when accessing the Internet and should not allow other staff to use their I.D.*

3.4. *When logged onto their Internet account members of staff should not leave a workstation unattended unless it is locked.*

The school will work with Agilysis and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved on a regular basis

If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator immediately (through the class teacher if appropriate).

Senior Management team in conjunction with the Computing Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

Managing emerging technologies

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

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
For additional information in this area please see the SAENCO and Child Protection policies
All information regarding children is kept centrally on the SIMS system and access to this system can only be granted by Agilysis services who allocate individual username and passwords. Currently the only members of staff who have access is the Head Teacher, two office managers.
Wherever possible, information concerning individual children including tests scores, data and IEP/IBP's can be found on the staff share system. Staff are advised to not put this information on removable drives or send via email systems due to data and child protection (see every child matters agenda).

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, Twitter, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or Twitter.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Policy Decisions

Authorising Internet access, Teams, Twitter and School Spider

All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

Parents will be asked to sign and return a consent form.

All staff must now undergo a two form authenticator process when logging into their Microsoft accounts from, new devices, this is verified by a certified pass number on a phone application to confirm identify. Tis will occur once every 60 days.

All children, staff and governors will be allocated a specific username and password under the condition that they must not be revealed to another pupil. If this should occur, the child or member of staff are no longer entitled to the username and password and the incident will be logged.

All parents must sign a consent form before children are allocated with a username and password.

Assessing risks

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. Neither the school nor St Helens filtering can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff, ideally the Head Teacher when available.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (See child protection policy)

Parents and pupils will need to work in partnership with staff to resolve issues.

Communications Policy

Introducing the online safety policy to pupils

Online safety rules will be posted in all networked rooms with Internet access and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.

Staff and the online safety policy in conjunction with St. Helens

In conjunction with the St. Helens LA Internet policy, has adopted the following actions:

3.6. *Members of staff should not use, or try to use, a school Internet account for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to School policy.*

3.7. *Where access to such sites occurs accidentally this should be immediately reported to the Head Teacher or, in the case of the Head Teacher being absent, a member of the Senior Management team.*

3.8. *Members of staff must be aware of, and abide by, the Data Protection Act as its provisions cover data transmitted and stored on e-mail. (See the Data Protection Policy and Code of Practice for further details).*

All staff will be given the School e-Safety Policy and its importance explained. This policy will be kept on Staff Share and edit on an annual basis.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.

Enlisting parents' support and advice for website.

Parents' attention will be drawn to the school e-Safety Policy in newsletters, and the website

Parent classes will be made available for Parents to fully understand the Internet risks and what they can do to prevent them.

Internet issues will be handled sensitively, and parents will be advised accordingly.

Communications	Staff and other adults				Students/pupils			
A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages: **Communication Technologies during school times**	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		✓						✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices eg tablets, gaming devices	✓					✓		
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails	✓							
Use of messaging apps	✓							✓
Use of social media			✓					✓
Use of blogs	✓					✓		

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff pupils or parents / carers (email, chat, blog etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school / academy* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in personal social media to students / pupils, parents / carers 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 local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school's* use of social media for professional purposes will be checked regularly by the head teacher and e-safety committee to ensure compliance with the social media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

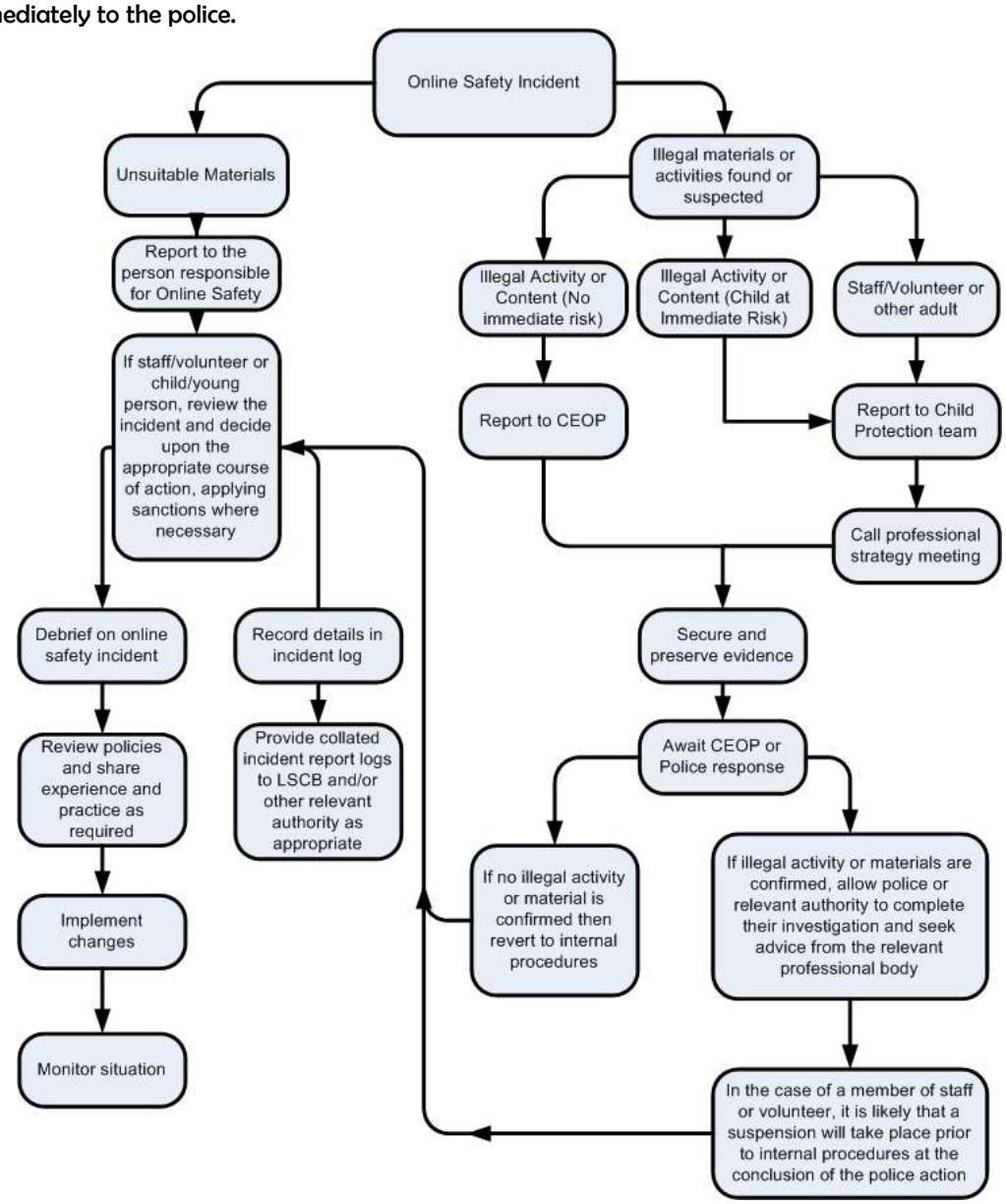
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)				X		
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing				X		
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting eg Youtube				X	X	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

• Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
• Internal response or discipline procedures
• Involvement by Local Authority or national / local organisation (as relevant).
• Police involvement and/or action
• If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
• incidents of 'grooming' behaviour
• the sending of obscene materials to a child
• adult material which potentially breaches the Obscene Publications Act
• criminally racist material
• other criminal conduct, activity or materials
• Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

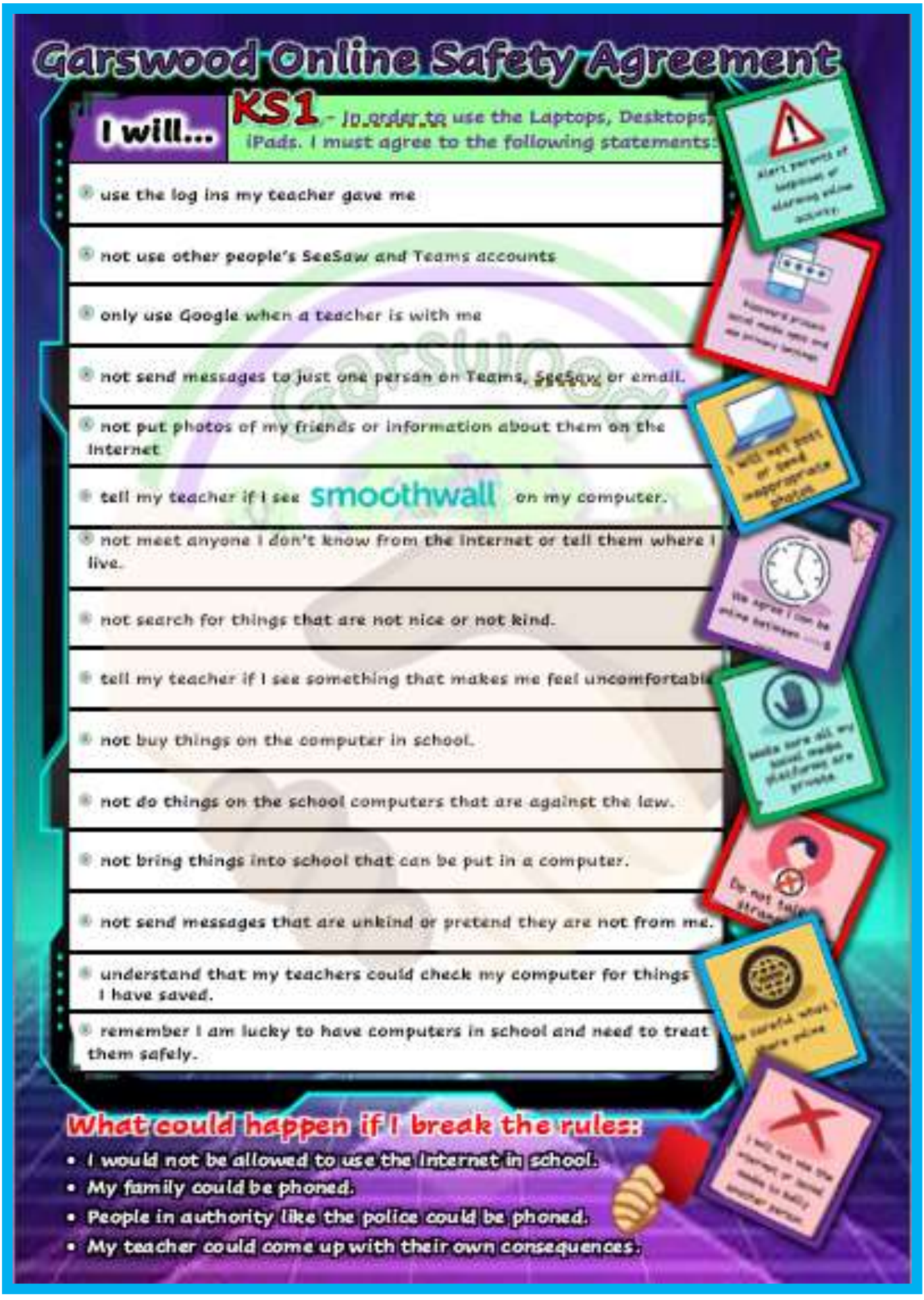
School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Incidents:	Inform Safeguarding Unit	Refer to Phase Leader	Refer to Headteacher /	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Consider Management instruction/warning processes	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X		X	X		X			
Unauthorised use of non-educational sites during lessons		X				X		X	
Unauthorised use of mobile phone / digital camera / other mobile device			X			X		X	
Unauthorised use of social media / messaging apps / personal email			X		X	X		X	
Unauthorised downloading or uploading of files			X		X	X		X	
Allowing others to access school network by sharing username and passwords			X		X	X		X	
Attempting to access or accessing the school / network, using another student's / pupil's account		X			X	X		X	
Attempting to access or accessing the school / academy network, using the account of a member of staff			X		X	X		X	X
Corrupting or destroying the data of other users			X			X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X		X	
Continued infringements of the above, following previous warnings or sanctions			X			X	X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X		X	X
Using proxy sites or other means to subvert the school's / filtering system	X		X	X		X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X		X	X	X		X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act/GDPR			X		X	X	X	X	X

Year	Be Sharp	Be Alert	Be Secure	Be Kind	Be Brave
3 Google Internet Legends	Activity 1: Is it ok to share? See page 9 and 53 in PDF Activity 2: Keeping it private See page 13 and 54 in PDF Activity 3: Interland: Mindful Mountain	Activity 1: Don't bite that phishing hook! See pages 18-21 and 54 in PDF Activity 2: Interland: Reality River See page 27 in PDF	Use baseline activity page 57 as guidance. Activity 1: How to build a strong password See pages 31-33 and 58 in PDF Activity 2: Taking care of yourself and others See page 36 and 59 in PDF Activity 3: Interland: Tower of Treasures See page 37 for discussion prompts	Could use 'Be a kindness superhero' on page 59. Activity 1: How can I stand up to others? See pages 41-42 and 60 in PDF Activity 2: Reacting to role-models See page 46 and 60 in PDF Activity 3: Interland: Kind Kingdom See page 47 for discussion prompt	Recap on the four pillars looked at over the first two terms. The last pillar is 'Be Brave' – what might this mean in the context of our lessons? How can you be brave with your online activity?
4 SWGFL	Year 4 – Rings of Responsibility lesson	Year 4 – The Key to Key Words	Year 4 – Private and Personal Information	Year 4 – The Power of Words	Recap on the four pillars looked at over the first two terms. The last pillar is 'Be Brave' – what might this mean in the context of our lessons? How can you be brave with your online activity?
5 Google Internet Legends	Use baseline activity on page 62 of PDF. Activity 1: Whose profile is this anyway? See pages 10/11 and 63 in PDF Activity 2: How do others see us? See page 12 and 63 in PDF Activity 3: Interland: Mindful Mountain See page 14 in PDF Followed by discussion – question prompts within PDF	Use baseline activity on page 65 as prompt for discussion. Activity 1: Don't bite that phishing hook! See pages 18-21 and 66 in PDF Activity 2: Who are you, really? See pages 22-26 and 66 in PDF Activity 3: Interland: Reality River See page 27 in PDF Followed by discussion – question prompts within PDF	Activity 1: How secure is my password? Use website https://howsecureismypassword.net/ Start with an easy word/phrase and develop using upper/lowers/numbers/characters to see what the strongest password they can create is. Activity 2: Shh...Keep it to yourself! We can't actually demonstrate this but the concept of privacy settings, 2-step verification can be discussed using info on page 34 and 70 in PDF Activity 3: Interland: Tower of Treasures See page 37 for discussion prompts	Use baseline activity page 72 as guidance. Activity 1: Turning negative into positive See pages 43-44 and 73 in PDF Activity 2: Mixed messages See page 45 and 73 in PDF Activity 3: Interland: Kind Kingdom See page 47 for discussion prompts	Recap on the four pillars looked at over the first two terms. The last pillar is 'Be Brave' – what might this mean in the context of our lessons? How can you be brave with your online activity?
6 SWGFL	Year 6 – Talking Safely Online	Year 5 – Picture Perfect	Year 6 – Privacy Rules	Year 6 – What's cyberbullying?	Recap on the four pillars looked at over the first two terms. The last pillar is 'Be Brave' – what might this mean in the context of our lessons? How can you be brave with your online activity?

Garswood Pupil requirements for Internet use KS1:



Garswood Pupil requirements for Internet use KS2:

Garswood Online Safety Agreement

I will...

In order to use the Laptops, Desktops, iPads. I must agree to the following statements:

- only access the computers and various applications with my own login and password, which I will keep secret. (Unless instructed by my teacher)
- not access other people's files, SeeSaw accounts or Teams log ins and damage their work.
- use the Internet when supervised with permission and only for activities and work approved by a member of staff.
- only Email people my teacher has approved, and not use the Internet , SeeSaw or Teams for personal or private messages.
- respect the privacy of others. I will not publish their names, addresses, phone numbers or photographs
- report a Smoothwall notification to a member of staff immediately and inform them of what I was inputting.
- not give my home address or telephone number, or arrange to meet someone, through the Internet
- not try to find or use unacceptable material from the Internet and not use work from the Internet as if it was my own
- report any unkind messages. I understand this report might be shared with responsible adults and would help protect pupils & myself
- not use school computers or iPads to subscribe to purchase any apps, or buy things off the Internet.
- not take part in any activity which goes against school rules or government legislation such as downloading online software.
- not bring in CD's, USBs or any electronic data from outside school unless I have been given permission
- not send unsuitable email messages. The messages I send will be polite, responsible and only signed in my name and not be anonymous.
- understand that the school may check my computer files and folders and may monitor the sites I visit e.g. SeeSaw and Teams.
- remember that access is a privilege, not a right and that access requires responsibility.

Sanctions – A breach of this may lead to these consequences:

- A temporary or permanent ban on Internet use.
- Pupils' parents being contacted.
- Other external agencies being contacted.
- Other actions may be added in line with Garswood's behaviour policy.

Garswood Curriculum Map coverage 2021 – Online Safety:

Online safety coverage – Year 1

KS1	Using Technology (IT)	Algorithms (IT)	Uses of IT beyond School (IT)	Create Programs (CS)	Safe Use (DL)	Reasoning (IT)
	Pupils should be taught to use technology purposefully to create, organise, store, manipulate and retrieve digital	*Pupils should be taught to understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions*	*Pupils should be taught to recognise common uses of information technology beyond school*	*Pupils should be taught to create and debug simple programs*	*Pupils should 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 should be taught to use logical reasoning to predict the behaviour of simple programs*
National Curriculum statement for KS1	*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.*					

	Sequence Taught	Digital Literacy Taught	How this will be taught
1:1	Mouse, keyboard and Images	Y1 Online Safety Twinkl e safety unit (and Curriculum Map resources)	*In this unit, children learn about the potential dangers in the online world and what basic steps we all need to take in order to have positive digital experiences. The first lesson, which is intended to be taught at the start of the school year, focuses on why it is important for children to name their creative work. They go on to learn about using a search engine safely to find pictures. Children learn the SMART rules and look at what information should be kept safe when using the Internet. The lessons then explore the positives and potential negatives of online communication, such as email, and children will develop the skills to recognise potential dangers and act accordingly to keep themselves and others safe*
1:2	Completing Online labels	Project Evolve Managing Online information Health and wellbeing online	• Strategies for effective searching, critical evaluation and ethical publishing • The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them. *The pupils need to consider copyright when sourcing images for their programs and/or uploading their own work to the Scratch community site. Searching for content for programs or viewing others' cartoons also offers an opportunity to develop safe search habits. If the pupils participate in the Scratch community, they need to think about what information they can share and how to participate positively in an online community, as well as obtaining parental permission.*
2:1	What is an algorithm?	Project Evolve privacy and security copyright and ownership	• Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise. • Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution. *The pupils consider how to stay safe while researching online and show respect for others' ideas and intellectual property by citing their sources and using licensed images. Safe search filters are in place for using Google and school internet access is filtered*
2:2	Music for Lovelace and Turing	Project Evolve self-image and Identity Online relationships	• Shaping online identities and how media impacts on gender and stereotypes • Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice. *Children will learn basic computer skills and learn to use effective passwords including Teams log ins*
3:1	Decisions, decisions	Think U Know scheme of work (and curriculum map resources) iLearn 2 e safety	*A series of videos and resources to help teach e-safety to Years 1 and 2 – there are also key questions in bullet points. We suggest covering videos 1-3 with Year 1 and finishing with the Lee and Kim video, then starting with Lee and Kim for Year 2 and moving onto videos 4-6. We have created a pupil activity pack with the videos and questions below for pupils/parents to access at home or school.* Pupil Activity Code: 42Q2
3:2	Can you spot a pattern?	Project Evolve Online reputation Online Bullying	• Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles • Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation *Pupils learn that everything they do online leaves a trail, culminating in their digital footprint. They discover the use of safe search modes or child friendly search engines and learn what to do if they meet inappropriate content. They also become familiar with intellectual property rights, including Creative Commons Licenses, and the importance of acknowledging other people's work.*

Online safety coverage – Year 2

KS1	Using Technology (IT)	Algorithms (IT)	Uses of IT beyond School (IT)	Create Programs (CS)	Safe Use (DL)	Reasoning (IT)
	Pupils should be taught to use technology purposefully to create, organise, store, manipulate and retrieve digital	*Pupils should be taught to understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions*	*Pupils should be taught to recognise common uses of information technology beyond school*	*Pupils should be taught to create and debug simple programs*	*Pupils should 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 should be taught to use logical reasoning to predict the behaviour of simple programs*
National Curriculum statement for KS1	*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.*					

	Sequence Taught	Digital Literacy Taught	How this will be taught
1:1	Animation	Project Evolve Managing Online information Health and wellbeing online	• Strategies for effective searching, critical evaluation and ethical publishing • The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them. *The pupils need to consider copyright when sourcing images for their programs and/or uploading their own work to the Scratch community site. Searching for content for programs or viewing others' cartoons also offers an opportunity to develop safe search habits. If the pupils participate in the Scratch community, they need to think about what information they can share and how to participate positively in an online community, as well as obtaining parental permission.*
1:2	Pictograms	Project Evolve privacy and security copyright and ownership	• Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise. • Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution. *The pupils consider how to stay safe while researching online and show respect for others' ideas and intellectual property by citing their sources, and using licensed images. Safe search filters are in place for using Google and school internet access is filtered*
2:1	Creating an Online e book	Project Evolve self-image and Identity Online relationships	• Shaping online identities and how media impacts on gender and stereotypes • Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice. *Children will revise basic computer skills and learn to use effective passwords and take screenshots*
2:2	Scratch Jr	Y2 Online Safety Twinkl e safety unit (and Curriculum Map resources)	*In this unit, children learn about how what they do online leaves a trail called a digital footprint. They will look at how to improve the efficiency of their online searches, the types of websites that are best for children to access when looking for information, as well as how to identify inappropriate content and the actions they should take if they do. Children will be introduced to the term 'cyberbullying' and look at how they should communicate online and deal with instances of people being unkind via digital means.*
3:1	Wonders of the Digital World	Think U Know scheme of work (and curriculum map resources) iLearn 2 e safety	*A series of videos and resources to help teach e-safety to Years 1 and 2 – there are also key questions in bullet points. We suggest covering videos 1-3 with Year 1 and finishing with the Lee and Kim video, then starting with Lee and Kim for Year 2 and moving onto videos 4-6. We have created a pupil activity pack with the videos and questions below for pupils/parents to access at home or school.* Pupil Activity Code: 42Q2
3:2	Tim Berners Lee Technology	Project Evolve Online reputation Online Bullying	• Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles • Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation *Pupils learn that everything they do online leaves a trail, culminating in their digital footprint. They discover the use of safe search modes or child friendly search engines and learn what to do if they meet inappropriate content. They also become familiar with intellectual property rights, including Creative Commons Licenses, and the importance of acknowledging other people's work.*

Online safety coverage – Year 3

KS2	Create programs (IT)	Develop programs (CS)	Reasoning (IT)	Networks (CS)	Search engines (IT)	Using programs (IT)	Safe use (DL)

National Curriculum statement for KS2 — Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

	Sequence Taught	Digital Literacy Taught	How this will be taught
1:1	Solving Steve Jobs Problem	**Project Evolve** Managing Online information Health and wellbeing online	• Strategies for effective searching, critical evaluation and ethical publishing • The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them. *The pupils need to consider copyright when sourcing images for their programs and/or uploading their own work to the Scratch community site. Searching for content for programs or viewing others' cartoons also offers an opportunity to develop safe search habits. If the pupils participate in the Scratch community, they need to think about what information they can share and how to participate positively in an online community, as well as obtaining parental permission.*
1:2	Gaming online friends and Privacy	**Internet Legends** scheme of work (and curriculum map resources) **iLearn 2 e safety**	**Be Internet Secure:** • Explain why it's important to keep personal information private online. • Describe ways to keep personal information private online by using safety tools and privacy settings. • Describe how to find and ask for help if someone feels unsafe online. **Be Internet Kind** • Demonstrate ways to build positive and healthy online relationships and friendships. • Describe strategies they can use to respond to hurtful online behaviour, in ways that keep them safe and healthy. • Identify sources of support that can help friends and peers if they are experiencing hurtful behaviour online.
2:1	Perfect Poetry	**Project Evolve** privacy and security copyright and ownership	• Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise. • Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution. *The pupils consider how to stay safe while researching online and show respect for others' ideas and intellectual property by citing their sources, and using licensed images. Safe search filters are in place for using Google and school internet access is filtered*
2:2	Digital Art and Music	**V3 Online Safety** Twinkl e safety unit (and Curriculum Map resources)	*In this unit, children are introduced to email and other forms of online communication. They will look at how to write and send emails, as well as how to decide if an email is safe to open. They will build on their existing knowledge of cyberbullying and how to deal with unkind behaviour online. The use and importance of privacy settings is introduced and children will discuss the types of information we should not share online. They will build on the idea of a digital footprint by thinking about how the adverts they see online are targeted at them. Children will finish the unit by using the knowledge they have gained to plan a party using online communication methods.*
3:1	Scratch Tunes	**Project Evolve** self-image and Identity Online relationships	• Shaping online identities and how media impacts on gender and stereotypes • Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice. *Children will revise basic computer skills and learn to use effective passwords and take screenshots*
3:2	Comic Creations	**Project Evolve** Online reputation Online Bullying	• Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles • Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation *Pupils learn that everything they do online leaves a trail, culminating in their digital footprint. They discover the use of safe search modes or child friendly search engines and learn what to do if they meet inappropriate content. They also become familiar with intellectual property rights, including Creative Commons Licenses, and the importance of acknowledging other people's work.*

Online safety coverage – Year 4

KS2	Create programs (IT)	Develop programs (CS)	Reasoning (IT)	Networks (CS)	Search engines (IT)	Using programs (IT)	Safe use (DL)

National Curriculum statement for KS2 — Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

	Sequence Taught	Digital Literacy Taught	How this will be taught
1:1	Animated Food Chain	**Project Evolve** self-image and Identity Online relationships	• Shaping online identities and how media impacts on gender and stereotypes • Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice. *Children will revise basic computer skills from year 3 and be reminded of the importance of using an effective password.*
1:2	TED Talks	**Project Evolve** Online reputation Online Bullying	• Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles • Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation *In filming one another, the pupils need to ensure that the appropriate permission has been obtained, and that they act respectfully and responsibly when filming, editing and presenting their work. The pupils should think through the implications of videos being made available on the school network or more widely via the Internet. They should discuss why schools and other organisations have strict policies over filming.*
2:1	Password and E safety	**Internet Legends** scheme of work (and curriculum map resources) **iLearn 2 e safety**	**Be Internet Secure:** • Explain why it's important to keep personal information private online. • Describe ways to keep personal information private online by using safety tools and privacy settings. • Describe how to find and ask for help if someone feels unsafe online. **Be Internet Kind** • Demonstrate ways to build positive and healthy online relationships and friendships. • Describe strategies they can use to respond to hurtful online behaviour, in ways that keep them safe and healthy. • Identify sources of support that can help friends and peers if they are experiencing hurtful behaviour online.
2:2	Mindset of Minecraft	**Project Evolve** Managing Online information Health and wellbeing online	• Strategies for effective searching, critical evaluation and ethical publishing • The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them *The pupils learn how easy it is to create content for the web. The unit provides an opportunity to address some of the risks of using the web, and how pupils could best keep themselves safe while doing so. They learn how easily web pages can be modified, which provides an opportunity to consider the reliability of web-based content.*
3:1	Rising to Bill Gates challenge	**V4 Online Safety** Twinkl e safety unit (and Curriculum Map resources)	*In this unit, children learn about preventing and dealing with cyberbullying; how to use search engines efficiently; how to avoid plagiarism online; and how to be a good digital citizen. The unit ends with children applying their new knowledge to design a character to be displayed around school to promote online safety.*
3:2	Choose your Team	**Project Evolve** privacy and security copyright and ownership	• Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise. • Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution. *The pupils consider the importance of obtaining and using accurate data for any information-processing work. If the pupils film one another, they need to ensure appropriate permission is obtained and that recordings are made, edited and shown in safe, respectful and responsible ways. The pupils should think carefully about the implications of uploading their films to the school network or to the Internet.*

Online safety coverage – Year 5

KS2	Create programs (IT)	Develop programs (CS)	Reasoning (IT)	Networks (CS)	Search engines (IT)	Using programs (IT)	Safe use (DL)
National Curriculum statement for KS2	Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.						

	Sequence Taught	Digital Literacy Taught	How this will be taught
1:1	Kodu Creations	Y5 Online Safety Twinkl e safety unit (and Curriculum Map resources)	*In this unit, children will learn about email safety with a focus on preventing and dealing with spam. They will consider the importance of strong passwords and learn how to create them. Children will build on their knowledge of plagiarism and fair use of people's work by learning how to write citations and references for websites they may use. They will [illegible] photographs that they see online and learn how easy it is to manipulate pictures and present them as reality.*
1:2	Networks and Inputs	Project Evolve Online reputation Online Bullying	• Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles • Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation *The unit provides an opportunity to reinforce messages around safe searching and evaluating the quality of online content. If the pupils upload their work for others to see, they should consider the importance of protecting personal information as well as recognising that they are sharing their own copyrighted work with an audience.*
2:1	CBeebies e book challenge	Project Evolve privacy and security copyright and ownership	• Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise. • Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution. *The pupils need to think about copyright when sourcing audio or publishing their own compositions. They are encouraged to use Creative Commons licensed content if working with others' audio files. There's an opportunity to discuss how copyright relates to music performed in school as well as illegal downloading and sharing of copyrighted music.*
2:2	Tour of America	Project Evolve Managing Online information Health and wellbeing online	• Strategies for effective searching, critical evaluation and ethical publishing • The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them *Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*
3:1	Preparing for the Planets	Project Evolve self-image and Identity Online relationships	• Shaping online identities and how media impacts on gender and stereotypes • Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice. *The pupils should observe good practice when searching for and selecting digital content. If the pupils choose to locate their 3D model geographically, they should avoid sharing private information. The pupils should think about copyright when adding content to their model or publishing images or videos of their model.*
3:2	Cyberbullying and Reporting	Internet Legends scheme of work (and curriculum map resources) iLearn 2 e safety	Be Internet Sharp: Explain what it means to have a positive digital footprint, and why it is important. • Explain things someone can do to build a positive digital footprint. Be Internet Alert Describe ways to critically evaluate what we see on social media • Explain how social media can mislead or misrepresent reality. • Identify different types if online scam people our age may experience including phishing Identify sources of support for someone who is worried about anything online.

Online safety coverage – Year 6

KS2	Create programs (IT)	Develop programs (CS)	Reasoning (IT)	Networks (CS)	Search engines (IT)	Using programs (IT)	Safe use (DL)
National Curriculum statement for KS2	Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.						

	Sequence Taught	Digital Literacy Taught	How this will be taught
1:1	Virtual Reality	Project Evolve self-image and Identity Online relationships	• Shaping online identities and how media impacts on gender and stereotypes • Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice. *The pupils create short videos. They learn the importance of observing school policy in relation to videoing, and the need to obtain consent. They think carefully about the implications of sharing content publicly on sites such as YouTube and consider how such publication would limit what they might include in their content. They recognise the need to use video search platforms in restricted or education specific modes and brainstorm what they should do if they encounter inappropriate content. They learn to respect the intellectual property rights of others, and the need to observe licence terms for any content they do not create themselves.*
1:2	History and Binary	Project Evolve Online reputation Online Bullying	• Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles • Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation *The pupils consider the capabilities of smartphones and tablet computers, and how these can be used purposefully. They become aware of some of the capabilities of these devices, including how they can be used to record and share location information, they consider some of the implications of this. They use search engines safely and effectively. The pupils could make use of their own tablets or smartphones in school, considering how they can do this safely and to good effect*
2:1	The Code behind the game	Project Evolve privacy and security copyright and ownership	• Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise. • Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution. *The pupils learn about some common algorithms, recognising that more efficient solutions to the same problem can reduce the impact of computation on energy and other resources. They remix code on Scratch and Snap! websites, as permitted by Creative Commons licences for the code they work with, in much the same way as they might modify open-source software. Pupils who wish to register for accounts on these sites need to observe the associated terms and conditions, which typically require parental consent.*
2:2	Emojis and communication Text talk/ Phishing	Internet Legends scheme of work (and curriculum map resources) iLearn 2 e safety	Be Internet Secure: Explain why it's important to keep personal information private online. Describe ways to keep personal information private online by using safety tools and privacy settings. Describe how to find and ask for help if someone feels unsafe online. Be Internet Kind Demonstrate ways to build positive and healthy online relationships and friendships. Describe strategies they can use to respond to hurtful online behaviour, in ways that keep them safe and healthy. Identify sources of support that can help friends and peers if they are experiencing hurtful behaviour online.
3:1	Programming with Python	Project Evolve Managing Online information Health and wellbeing online	• Strategies for effective searching, critical evaluation and ethical publishing • The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them *The pupils create a school magazine or yearbook. They think carefully about the implications of including photographs of pupils in their work, recognising that typically names would not be used in captions and that they should have permission to publish any pictures they use. They respect school policies and relevant legislation. They also recognise that intellectual property exists in other pupils' work and that this should be respected, so include such example only with permission. They also learn that sensitive personal information should not be included in publications such as these, thinking carefully about what this means in practice*
3:2	Image Editing	Y6 Online Safety Twinkl e safety unit (and Curriculum Map resources)	*In this unit about online safety, children will be taking a more in depth look at a variety of online safety issues, most of which they will have been familiarized with in previous years. They will be introduced to the idea of the internet, as a type of media, and how it can shape our ideas about boys and girls through stereotypes. Children will be given ways to deal with online content that they find worrying or even believe to be dangerous*

Online safety coverage – EYFS

National Curriculum statement for KS1	*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.*

Sequence Taught	Digital Literacy Taught	How this will be taught
EYFS will not be teaching e safety as part of a half termly approach. E safety resources opposite will provide Foundation Stage staff with all the tools necessary to ensure children are fully aware teaching e safety in accordance with the children' s interests.	**Think U Know** scheme of work (and curriculum map resources)	*Early years' children will not naturally be aware of the dangers of the internet because their use of it will be minimal compared to older children. It is still very important to introduce positives and the negatives as it does form part of the EYFS framework. Below are some activities and resources you can use with the children, which also form nice discussion points. In many ways on-line safely can be connected to general safety discussions; not talking to strangers, if something is wrong tell an adult you trust etc.*
	iLearn 2 e safety **Project Evolve** • Managing Online information • Health and wellbeing online • privacy and security • copyright and ownership self-image and Identity • Online relationships Online reputation • Online Bullying **Internet Matters** EVFS Pack **Twinkl resources** Early Years e safety	**Resources for settings to use with parents and carers** • AskAboutGames: Supporting families with video games • Childnet: Keeping under-fives safe online • Internet Matters: Guidance for parents of pre-schoolers • London Grid for Learning: Portal linking to various resources on parental engagement around online safety • NSPCC: Guidance for parents on keeping children safe online • Parent Zone: Digital Parenting magazine • Parent Info • Thinkuknow: Guidance and information for parents/carers from NCA-CEOP **Resources for settings to use for education** Childnet: Storybooks for early years and KS1 pupils • Smartie the Penguin • Digiduck Stories Thinkuknow - Resources for early years and KS1 pupils from NCA-CEOP UKCIS - Education for a Connected World' Framework - this framework provides information on the skills and competences that children should have across 8 different areas of online safety **Cheadin** *The do and don'ts for Early Years online safety:* According to Ofcom's recent survey on Children's Media Use and Attitude (2018), 52% of 3-4-year-olds use the internet for an average of 9 hours every week and 45% 3-4-year-olds use YouTube. With technology becoming an integral part of our lives, it's important that children are familiarised with safe online practice from a young age. Apart from supervision, guidance and monitoring, it's also the responsibility of carers to set the right example for safe usage and privacy awareness

Computing Lead - Les Moon June 2023