Online Safety and Acceptable Use Policy

Policy Title	E-Safety and Acceptable Use Policy
Statutory	Yes
Policy Version	4
Policy Author	Mrs E Cameron
Ratified By	FGB
Date Ratified	Autumn 2022
Review Period	2 years
Next Review Period	Autumn 2023
Distributed To	All Staff/Parents/Governors
To be published on website	Yes
Changes to this policy	V4- New policy to replace e-safety policy Previous e-safety policy acceptable use included as an appendix (appendix 4). This has been updated to make correct reference to SeeSaw and Teams. V3- Wording updated in E-Safety Rules for Key Stage 2 – page 12
This policy has been impact assessed against race, gender and disability and no adverse impact has been identified.	

Contents

1. Aims

Carrington Junior School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education]
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and assistant DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, computing co-ordinator and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy

- Ensuring that any online safety incidents are logged (on Cpoms) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager (Turn It On)

The ICT manager (Turn It On), in collaboration with school leadership, is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged, communicated to school leadership, and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

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

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools

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

The safe use of social media and the internet will also be covered in other subjects where relevant and appropriate, including but not exclusive to PSHE and English (where pupils will be taught to read critically for bias).

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, via SeeSaw or on Teams. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- That the school uses to filters and monitors online use

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. Cyber-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Pupils are taught about bullying as part of the PSHE curriculum**. We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Behaviour & Exclusions Policy.**

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 tutor groups.

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 (see section 11 for more detail).

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

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

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

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

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

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

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

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils are not permitted to have mobile phones in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However, we discourage this on security grounds as they are easily lost, damaged or stolen, although with written consent this can be made possible.

Pupils are taught that they should not have a mobile phone on their person in school and that any phone brought in must be handed to the appropriate person at morning registration to be stored in the office for the duration of the day, and should be collected by pupils at the end of the day.

Phones are brought into school at the pupil and parents own risk.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Using the installed anti-virus and anti-spyware software, and not bypassing it in any way
- Keeping operating systems up to date by always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Turn It On, the Finance Officer, the computing co-ordinator, or school leadership.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use . The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and assistant DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. Reports of incidents can be generated from Cpoms.

This policy will be reviewed every year by the headteacher and governors. At every review, the policy will be shared with the governing board. The review will consider and reflect the current risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer (I will not share images of myself or my home online either) • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Pretend to be anybody else online • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school (Year 5/6 with written permission to walk to school ONLY):** • I will make sure it is handed in to the appropriate person at the start of the day and collect it at the end of the day from the office **I agree that the school will monitor the websites I visit, and read messages that I post on school platforms, and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I agree to talk to my child about appropriate use of the internet at home, and monitor their use of the internet as appropriate for their age.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school may monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Acceptable use of internet and ICT

Acceptable Use of Internet by Staff

It is important that when members of school staff communicate with pupils they remember their professional role.

Communication between children and young people – by whatever method – should take place within clear and professional boundaries. This includes the wider use of technology such as mobile phones, text messages, emails, digital cameras, videos, web-cams, websites and blogs.

This means that staff should:

- *NOT* give their personal contact details to pupils, including their mobile telephone number or personal email address.
- *NOT* use the internet or web-based communication channels to send personal messages to pupils, outside of school apps such as SeeSaw and Teams.
- *BE AWARE* of information that they are putting into the public domain (Facebook, Twitter, etc.). Do *NOT* allow children or young people - associated with the school – to be listed as their 'friends' and Do *NOT* allow themselves to be listed as a 'friend' on their sites.
- *NOT* request or respond to any personal information from a pupil.
- *KNOW* that it is the legal responsibility of ALL members of staff to report child protection concerns and follow the school Child Protection Policy.

Email or text communications between a member of staff and a pupil may lead to disciplinary and/or criminal investigations. This also includes communications made through internet sites.

Use of Social Media

On Facebook or other internet communication: discussing school or referring to any child, staff member or groups of children is very unprofessional and against safeguarding and confidentiality practices.

No member of staff should ever allow a child or ex-pupil to become a 'friend' on Facebook or any similar website or mobile communications. This is a serious safeguarding issue.
Staff need to ensure their security settings are fixed carefully on Facebook, and other social media channels, as a lack of security could lead to parents or children knowing about personal matters could compromise professionalism.

Physical Safety

- All electrical equipment in the school is tested annually to ensure that it is safe to use.
  Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum. **We expect pupils to behave appropriately near electrical sockets and appliances.**
- Workstations are cleaned and sanitised regularly. Pupils are taught to avoid taking food and liquids anywhere near the computers. **We expect all users to refrain from eating and drinking when working at a computer.**
- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy. **We expect all users to take responsibility for their own physical well-being by adopting good practices.**
- Computers and other IT equipment can be easily damaged. Pupils are taught the correct way to use IT equipment. **We expect pupils to respect IT equipment and take care when handling and using.**

Network Safety

- All staff users need to log on using a unique username and password. Pupils log on with their personal login. Pupils are taught that they should only access the network using those particular logins. **We expect all users to only logon using their individual username.**
- Each user is given an allocation of storage for their work. Pupils

are taught how to save their work into their area. Carrington Junior School is moving to Teams and OneDrive storage during 2022-23. **We expect pupils to save and keep their work to build up a portfolio of evidence.**

- Access to other users areas are restricted by the network. Pupils are taught not to access another user's work without permission. **We expect pupils to respect the privacy of all other users and to make no attempt to access or interfere with another user's work.**
- On the network and Teams there are "shared resource" areas where many different groups of users can save work so that it is available to others. Pupils are taught how to access and save to these shared resource areas. **We expect pupils to respect the contributions of others, not to delete or alter others' work and to ensure that they only save work to shared areas with permission.**
- Each user has the capability to print their work. Pupils are taught to only print when necessary to save resources for financial and environmental reasons. **We expect pupils to only print out work when directed by staff to do so.**
- The network software prevents changes being made to computer settings. Pupils are taught that making changes may prevent the computer from working properly. **We expect all users to make no attempt to alter the way the computer is set up.**
- Only the network administrators are permitted to install software on to computers. Pupils are taught that the network or an application may not function properly if programs are installed. **We expect all users to make no attempt to load or download any program onto the network.**
- Pupils are taught that their use of the network can be monitored, and may result in the application of the behaviour policy. **We expect all users to understand that their use is subject to monitoring.**

Internet Safety

- When using a network workstation all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. However, no system is 100% safe and we expect users to behave responsibly. Pupils are taught that the internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or can damage your computer. **We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media.**
- Pupils accessing the internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. **We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the internet.**
- The school website contains school policies, newsletters and other information. **We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.**

Email & Seesaw Safety

- Pupils have access to Teams, which pupils can send homework or school- related questions to. The class teacher monitors the pupil's use of email and Teams. Pupils are taught that messages and emails sent to their class email should have a clear learning purpose and be written in a polite style which is appropriate to the person that will receive it. **We expect all users to communicate appropriately through email and on Teams.**
- Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore, we do not permit the use of personalised email accounts by pupils at school or at home for school purposes. Pupils are taught that using a personalised e-mail account in school or for school use is not permitted. **We expect pupils to use school issued email accounts only.**
- The majority of families are signed up to the Seesaw app and therefore have a communication link with class teachers. The class teacher will use Seesaw to: keep parents updated on children's work and progress, update the whole class on notifications, respond to parents' questions and to let parents know about homework that has been set.
- All communication will use a professional tone. Class teachers are expected to keep parents updated on their children's progress weekly, including sharing some pupils' work.

- **Important communication/ information will be copied to CPOMs so that SLT are aware. This is strictly confidential.**

Home Learning

- With the home-school communication now readily available, children should have immediate access to remote/home learning should the need for it come.
- Staff will ensure any home learning is accessible for all children – mainly online or by post in very rare circumstances.
- Any learning sent home should enable children to be as independent as possible to relieve extra pressure on parents/carers. This can include: teacher videos, Power-points with voice overs or being directed to specific websites – these websites must be checked and verified by staff before being sent out.
- Teachers will ensure communication with the class and have regular updates with families of vulnerable children.
- Staff will be available for contact via Seesaw during school hours.
- Any marking or feedback of home learning will follow the school marking policy.

Digital Images

- Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. On the website we never state the child's full name with their image (see policies regarding GDPR). **The school will happily remove any image of a child on the school website at their parents' request.**
- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff. Pupils are taught to seek permission before copying, moving, deleting or sending any images taken within school. **We expect all pupils to seek permission from staff before sharing images outside of the school environment.**

Other Technologies

- **Podcasting** – Some pupils will be given opportunities to create oral recordings. Some of these recording may be made available as podcasts through the internet so that they can be shared with interested members of the school community.

Copyright

- Though there are lots of free to use resources on the internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. Pupils are taught that the people who put their work on the internet may not always want people to copy or use their work and that they should check whether they have permission. **We expect all users to respect copyright laws.**
- It is important to know what work is original and when chunks of text have been copied from other sources such as the internet. Pupils are taught that they should not present the work of others as their own work. Older pupils are taught about copyright and how to extract or paraphrase information through appropriate referencing. **We expect all pupils to make it clear what is their own work and what is quoted from other sources.**

GDPR

- In line with GDPR guidelines, we must be transparent with regards to the information we hold about a child. When displaying a child's work, we must obey the guidelines (separate policy). When a child leaves the school, their Intellectual Property must be offered to them OR disposed of (again obeying the GDPR guidelines).