Baines' Endowed Church of England Primary Academy

Online Safety Policy

Our mission statement at Baines' Endowed Church of England Primary is:

"With God, nothing is impossible" Luke 1:37

To support our pupils, staff, parents and governors in their quest to achieve the 'impossible', we will teach, guide and nurture our community in the following twelve values:

generosity	compassion	courage	forgiveness
friendship	respect	thankfulness	trust
perseverance	justice	service	truthfulness

At Baines' Endowed, we believe that by valuing all God's children and teaching them to learn, develop and grow in the Gospel values, we will allow them the opportunity to believe that, with the help and love of God the Father, God the Son and God the Holy Spirit, they can achieve what they aim to achieve.

Refer also to;

- ICT/Computing Policy
- Acceptable Use Agreements
- Safer Working Practices Policy
- Pastoral Care and Child Protection Policy
- Behaviour Management Policy
- Anti-Bullying Policy
- PSHE Policy
- Computing Curriculum
- Safer Children in a Digital World

Introduction

At Baines' we believe that the use of information and communication technologies in school brings great benefits to both children and staff. Recognising the online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications, therefore keeping children and staff safe.

Our Online Safety Policy has been written building on the Blackpool Council e–Safety Policy, Cidari policy, government guidance and E360 safe recommendations. This policy applies to all members of the academy community (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of the school. All staff and volunteers sign to say they have read, understood and will comply with the Online Safety Policy as part of the staff contract/volunteer agreement signed when employment/placement begins. All staff and volunteers will also sign an acceptable use agreement.

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 academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy.

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 published Behaviour Management Policy. The academy 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 online behaviour that take place out of school.

Online safeguarding, as with any form of safeguarding, is **everyone's** responsibility.

Why use the internet?

Internet use can be part of the curriculum and a tool for learning. It is a part of everyday life for education, business and social interaction. Pupils and staff use the internet widely outside of the academy and need to learn how to evaluate internet information and to take care of their own safety and security.

The purpose of internet use in the academy is to raise educational standards, to support the professional work of staff and to enhance the management functions.

Benefits of using the internet include:

- Access to world-wide educational resources including museums and art galleries; Educational and cultural exchanges between pupils world-wide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of settings, support services and professional associations;
- Access to learning wherever and whenever convenient.

Internet access in the academy is planned to enhance and extend learning. As such, pupils will have access to a variety of devices for educational purposes. Any devices from the academy that are able to be used at home for out of hours learning should be used for the purposes of education only and by the pupil it is assigned to. Users must abide by academy policies about online safety.

Portable data devices (flash drives etc) must not be used in academy devices. Pupils will be informed about the online safety policy, what internet use is acceptable and what is not and given clear objectives for internet use from Reception through to Year 6. Pupils and their parents will be required to sign an acceptable use agreement as part of the induction process and Home/School Agreement before starting at the academy. Pupils will also learn about and sign to comply with the AUA at the beginning of each academic year.

Access levels to the internet will be reviewed to reflect learning requirements and age of pupils. Staff will guide pupils to 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.

Any copying and use of Internet derived materials by staff and pupils will comply with copyright law. Pupils and staff will be taught to respect copyright when using Internet material.

Maintaining Information Systems Security

- The security of the academy information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed to be attached to email.
- Files held on the academy network will be checked regularly.
- The Network Manager will review system capacity regularly.

Managing Email

- Staff may only use academy email accounts to send/receive academy related information.
- Staff must tell the Headteacher if they receive an offensive email.
- Access to external personal email accounts may be blocked. Staff must not access personal email on their own devices during their directed work time.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on setting headed paper.
- The forwarding of chain messages is not permitted. It is not permitted to send emails in capital letters - this can be intimidating, rude and is considered as shouting at the recipient.
- It is not permitted to send messages that are, or could be perceived as aggressive, abusive, threatening, obscene, defamatory, racist, sexist, discriminatory, pornographic, offensive or otherwise inappropriate.
- The reporting of child protection/ wellbeing issues of the children will be sent securely and sent as confidential email.
- Staff should only use specific email accounts to communicate with parents as approved by the Senior Leadership Team. Google hangouts - parents/carers can access email addresses through this however they will be reminded that any e-mail communication should come through the main admin address.

Publication of Information, Pupil Images/Work

- The contact details on the website should be the address, email and telephone numbers of the academy.
- Staff or pupils' personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT').
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Images that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Permission from parents or carers will be obtained before images of pupils are electronically published.
- Pupils' work can only be published with their permission and that of their parents/carers.

Social Media/Networking

- Access to social media and social networking sites is forbidden during directed working hours and whilst using academy devices unless for approved academy purposes.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, setting attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Staff and pupils must not place photos from events at the academy on any social network space (excluding academy pages/accounts).
- Parents/carers must not place photos that show other children apart from their own from academy events on social media
- Advice will be given regarding background detail in a photograph which could identify the pupil or his/her location.
- Staff official blogs or wikis should be password protected and run from the academy website with approval from the Senior Leadership Team.
- If personal publishing is to be used with pupils, then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site will be moderated by staff.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Staff are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. This includes from their own home network if it involves anyone (staff, parent or child) from the academy.
- The use of academy approved social media is permitted as a tool for communicating with parents/carers and the wider community. This will be monitored on a daily basis by a designated member of staff (Mrs Debi Rusling) to ensure appropriate content for the purpose of safeguarding alongside information giving. There will be limitations to external contributions again to ensure appropriate content.

Filtering

- Blocking strategies prevent access to unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day. This limits pupils' and staff access to a narrow range of information.
- Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- Keyloggers record all text sent by a workstation and analyse it for patterns. False positives will require manual checking.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Network Manager or a senior leader.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that is believed to be illegal must be reported to appropriate agencies such as CEOP/AWAKEN.
- Access will be designed by educators to suit the age and curriculum requirements of the pupils.

Video Conferencing

- All video conferencing equipment in the setting must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name. (contact internet provider for details).
- External IP addresses should not be made available to other sites.
- Video conferencing contact information should not be put on the academy website.
- The equipment must be secure and if necessary locked away when not in use. Video conferencing equipment should not be taken off the premises without permission from the Head teacher.

Users

- Video conferencing should be supervised appropriately for the pupils' age.
- Parents and carers should agree for their children to take part in video conferences.
- Login and password details for the educational video conferencing services should only be used by members of staff and kept secure.

Content

- Video conferencing is a challenging activity with a wide range of learning benefits.
- Preparation and evaluation are essential to the whole activity.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a video conference. If it is a non-educational site, it is important to check that they are delivering material that is appropriate for the age and stage of the children.

Managing Technologies and Data

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use is allowed.
- Staff will use academy phones where contact with parents is required. In extreme circumstances it is at the discretion of the Head teacher to allow staff to use their own phones ensuring appropriate measures are in place to avoid the sharing of staff's personal numbers.
- Mobile phones will not be used during school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be;

o Fairly and lawfully processed

o Processed for limited purposes

o Adequate, relevant and not excessive

o Accurate

o Kept no longer than is necessary

o Processed in accordance with the data subject's rights

o Secure

o Only transferred to others with adequate protection.

- A record of all staff and pupils who are granted access to the setting's electronic communications is held by the head teacher/network manager.
- All staff must read and sign to agree understanding of the 'Safer Working Practices Policy" before using any ICT resource.
- In nursery, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents/Carers will be informed that pupils will be provided with supervised internet access.
- The setting will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via an academy computer.
- The academy cannot accept liability for the material accessed, or any consequences resulting from internet use. The academy should audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate.
- 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.
- Data regarding online safety incidents will be monitored on a termly and annual basis and inform subsequent reviews of the policy.

- CPD will be sought to ensure staff are trained appropriately to manage online safety.

Cyberbullying

- Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007
- Cyberbullying (along with all forms of bullying) will not be tolerated.
- All incidents of cyberbullying reported will be recorded through My Concern and will be investigated accordingly.
- Staff and parents/carers will be advised to keep a record of the bullying as evidence.
- Steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, will be taken if necessary.
- Sanctions for those involved in Cyberbullying may include:

o The bully being asked to remove any material deemed to be inappropriate or offensive.

o A service provider may be contacted to remove content.

o Internet access may be suspended at the setting for the user for a period of time.

o Parent/carers may be informed.

o The Police will be contacted if a criminal offence is suspected. (For inappropriate images call 101 and pass on information – remove the device with suspected inappropriate images – do not look at the images yourself)

- All users will be informed that network and internet use will be monitored.
- Pupil instruction in responsible and safe use should precede internet access.
- Safe and responsible use of the internet and technology will be reinforced across the school. Particular attention will be given where pupils or staff are considered to be vulnerable.
- The Online Safety Policy will be discussed with all members of staff.
- To protect all staff and pupils, the academy will implement Acceptable Use Agreements.
- 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 both professionally and personally will be provided.

Parent/Carer Involvement

- Parents’ attention will be drawn to the Online Safety Policy in the prospectus and on the website.
- A partnership approach with parents/carers will be encouraged. This includes information evenings with demonstrations and suggestions for safe home internet use or highlighting online safety at other attended events e.g. parent evenings, fun days.

- Information and guidance for parents/carers on online safety will be made available to parents/carers in a variety of formats.
- Further information will be available via links on the school website.

At Baines' we realise that online safeguarding is an issue that is wider than the academy community. It can spread into daily life outside of school hours and can cause further upset within the academy setting. We will support the pupils, parents/carers, staff and members of the community in dealing with the issues as far as we can however, it may be necessary to signpost to other services. This may be done by discussions with families or additional learning opportunities in school.

For pupils who do not abide by the online safety policy, there will be consequences such as those outlined below;

- Exclusion from the lesson
- Discussion with parents/carers
- Limiting of access to electronic devices

Incidents regarding online safety will be reported to the Pastoral Team and logged accordingly. Data will be analysed on a termly basis and subsequent provision reviewed in light of it.

Complaints

- Complaints of internet misuse will be dealt with under the academy Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- All online safety complaints and incidents will be investigated and dealt with appropriately.
- Any issues (including sanctions) will be dealt with according to the behaviour management and child protection procedures.
- Pupils and parents/carers will be informed of the complaints procedure.
- Parents/carers and pupils will work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Settings Partnership Co-ordinators and/or the First Response Unit to establish procedures for handling potentially illegal issues.
- The academy will be sensitive to internet related issues experienced by pupils and staff out of setting, e.g. social networking sites, and offer appropriate advice.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body (Lindsey Taylor) has taken on the role of Online Safety Governor.

The role of the Online Safety Governor may include:

- Regular meetings with the Online Safety Coordinator
- Regular monitoring of online safety concerns
- Regular monitoring of filtering / change control logs
- Reporting to relevant meetings

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the academy community, though the day to day responsibility for online safety will be delegated to the Online Safety Coordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.
- Ensure that photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

The Senior Leadership Team will receive termly monitoring reports from the Online Safety Coordinator or DSL.

Online Safety Coordinator - Jack Parkinson

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the academy online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority/relevant body.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meetings.
- Reports to the Senior Leadership Team.

Technical staff

The Technical Staff are responsible for ensuring:

- That the academy's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the academy meets required online safety technical requirements and any Local Authority/Cidari Online 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 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher/Senior Leader; Online Safety Coordinator for investigation and any subsequent actions.
- That monitoring software / systems (Securly) are implemented and updated by the technical team. Reports are received via e-mail to the DSL and highlight attempts at inappropriate internet usage.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices
- They have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- They report any suspected misuse or problem to the Headteacher / Senior Leader; Online Safety Coordinator for investigation and any subsequent actions.
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official academy systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and Acceptable Use Agreements
- 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 academy activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned 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
- Care is taken when taking digital / video images to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Designated Safeguarding Lead - Nicola Sawyer

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils

Are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Agreement

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile. devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of the academy and realise that the academy's Online Safety Policy covers their actions out of academy hours, if related to their membership of the academy.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, bulletins, letters, websites and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at academy events - In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images must not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the academy

Policy Statements - Education – Pupils

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience.

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
- A planned online safety curriculum should be provided as part of Computing / PSHCE / other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and PSHE activities.
- 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Staff should be aware of the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material 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 the academy. This will be done at the beginning of a child's Reception year and revisited each academic year in September.
- 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.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- 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 academy 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 e.g. on social networking sites.

Education – Parents / Carers

Some parents and carers have only a limited understanding of online 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/carers 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 academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities.
- Letters, bulletins, website.
- Parents / Carers evenings / Information sessions.
- High profile events / campaigns e.g. Safer Internet Day.
- Reference to the relevant websites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide online safety information for the wider community.

Education & Training – Staff / Volunteers

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

- Online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out annually.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

- The Online Safety Coordinator / Computing Lead or Technical Support Team will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association /NCSL or other relevant organisation (e.g. SWGfL).
- Participation in academy training / information sessions for staff or parents (this may include attendance at specific worships/assemblies/lessons).

Technical – infrastructure / equipment, filtering and monitoring

- The academy has a managed ICT service provided by a central contractor (Cidari IT Helpdesk), it is the responsibility of the Trust to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the academy, as suggested below. It is also important that the managed service provider is fully aware of the academy Online Safety Policy / Acceptable Use Agreements.
- The academy should also check their Local Authority / Cidari / other relevant body policies on these technical issues.
- The academy will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.
- Academy technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of academy technical systems by the Cidari central team.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users (EYFS, KS1 & KS2 and above) will be provided with a username and secure password by the computing lead who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at regular intervals. Teachers are aware of the associated risks.
- The “master / administrator” passwords for the academy ICT system, used by the Technical Staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe/lockable filing cabinet)
- The Trust Business Manager, along with the Computing Lead is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details) Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. Nb. additional duties for academies under the Counter Terrorism and Securities Act 2015 which requires academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on “appropriate filtering”).
- The academy has provided enhanced / differentiated user-level filtering allowing different filtering levels for different ages / stages and different groups of users – staff / pupils etc.
- The academy uses Securly to filter and monitor internet use.
- Users must report any actual / potential technical incident / security breach to the relevant person, usually a teacher or teaching assistant in the first instance, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data. These are tested regularly. The academy infrastructure and individual workstations are protected by up to date virus software.
- Policy for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the academy systems is in the process of being established.
- The academy Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

The School allows

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device1	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes *	Yes **	Yes **
Full network access	Yes	Yes	Yes			
Internet only						
No network access						

* Pupils leave these devices in the school office during the day.

**Not to be accessed when working with pupils or in areas not designated for personal use.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers benefit of using these technologies for education outweighs their risk / disadvantages:

	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times and with staff permission	Not allowed
Mobile phones may be brought to the school	x					x	
Use of mobile phones in lessons				x			x
Use of mobile phones in non-directed time (In staff room/PPA room/own office)	x						x
Taking photos on mobile phones / cameras		x					
Use of other mobile devices e.g. tablets, gaming devices		x				x	
Use of personal email addresses in school, or on school network in non-directed time		x					x
Use of school email for personal emails				x			x
Use of messaging apps – own devices		x					X
Use of messaging apps – school devices	x						X
Use of social media – own devices		x					X
Use of social media – school devices		x					x
Use of blogs		x				x	

- If the academy wifi is not being used, then usage will not be picked up by monitoring system

When using communication technologies, we consider the following as good practice:

- The official academy 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 academy email service to communicate with others when in the academy, or on academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy 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 and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online 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 academy 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/academies 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 / academy group liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the academy through:

- Ensuring that personal information is not published.
- Training is provided including: 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.
- Academy staff should ensure that: No reference should be made in social media to pupils, parents / carers or academy staff.
- They do not engage in online discussion on personal matters relating to members of the academy community.
- Personal opinions should not be attributed to the academy or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Where official academy social media accounts are established there should be:
- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including;

    o Systems for reporting and dealing with abuse and misuse

    o Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used it must not associate itself with the academy or impact on the academy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- Monitoring of Public Social Media may occur to ensure the above points are complied with.
- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the academy.
- The academy should effectively respond to social media comments made by others according to a defined policy or process.
- The academy's use of social media for professional purposes will be checked regularly by the senior leadership team to ensure compliance with the academy policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.
The academy believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in / or outside the academy when using academy equipment or systems. The academy 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
Promotion of extremism or terrorism					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	

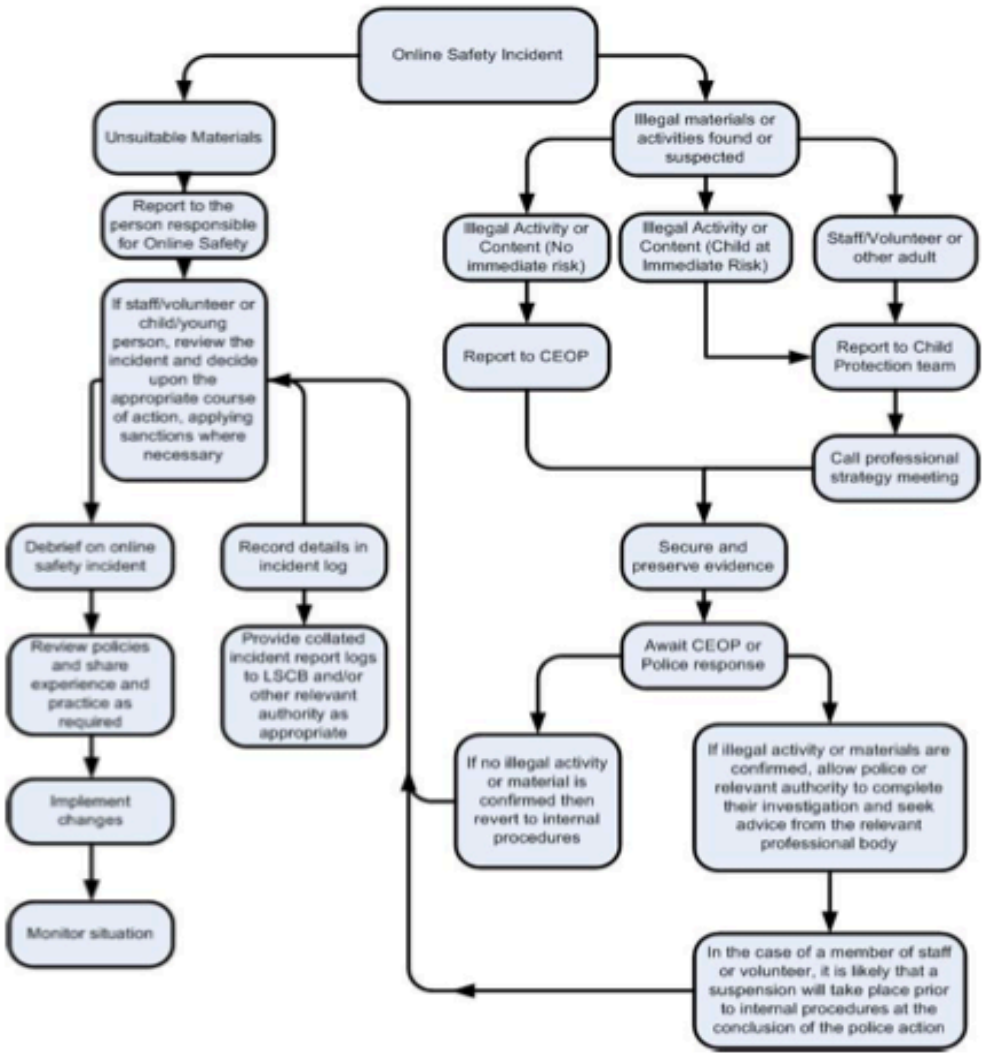
On-line gaming (educational)		X			
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce			X		
File sharing	X				
Use of social media		X	X		
Use of messaging apps		X	X		
Use of video broadcasting e.g. Youtube		X			

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 academy community will be responsible users of digital technologies, who understand and follow academy 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 it 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:
    - o Internal response or discipline procedures
    - o Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - o 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:
    - o Incidents of 'grooming' behaviour
    - o The sending of obscene materials to a child
    - o Adult material which potentially breaches the Obscene Publications Act
    - o Criminally racist material
    - o Promotion of terrorism or extremism
    - o 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 academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

It is more likely that the academy 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 academy 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:

Pupil Incidents	Refer to class teacher	Refer to KS 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	Warning	Further sanction such as 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	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X						X	
Unauthorised / inappropriate use of social media / messaging apps / personal email		X						X	
Unauthorised downloading or uploading of files		X			X			X	
Allowing others to access academy network by sharing username and passwords			X		X	X	X	X	
Attempting to access or accessing the academy network, using another pupil's account		X			X	X		X	
Attempting to access or accessing the academy network, using the account of a member of staff			X			X	X		
Corrupting or destroying the data of other users		X			X	X	X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X	X		
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the school			X			X		X	
Using proxy sites or other means to subvert the academy's filtering system			X		X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X			
Deliberately accessing or trying to access offensive or pornographic material			X			X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X		X	

** If repeated incidents of the same kind occur further sanctions than those marked above will be imposed at the discretion of the headteacher.

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Disciplinary action		
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		
Inappropriate personal use of the internet / social media / personal email		X					X		
Unauthorised downloading or uploading of files		X			X		X		
Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account	X				X	X			
Careless use of personal data e.g. holding or transferring data in an insecure manner		X					X		
Deliberate actions to breach data protection or network security rules		X			X		X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X		X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X					X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X					X		
Actions which could compromise the staff member's professional standing		X				X			
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		X					X		
Using proxy sites or other means to subvert the academy's filtering system		X					X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X		X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X			X		
Breaching copyright or licensing regulations		X					X		

**If repeated incidents of the same kind occur further sanctions than those marked will be imposed at the discretion of the headteacher.

Monitoring and Review

Should serious online safety incidents take place, the following external persons / agencies should be informed as appropriate:
LA Safeguarding Officer
Cidari (Peter Ashworth)
Police

Review

The academy will monitor the impact of the policy using:

- Logs from My Concern
- Monitoring logs of internet activity (including sites visited) / filtering Internal monitoring data for network activity
- Surveys / questionnaires of students / pupils / parents / carers / staff
- Scope of the Policy

Policy reviewed November 2024 by Mr J Parkinson (Computing Lead) and Miss N Sawyer (DSL)

Appendices

- Pupil Acceptable Use Agreement – KS2
- Pupil Acceptable Use Policy Agreement – EYFS / KS1)
- Staff (and Volunteer) Acceptable Use Policy Agreement
- Community/Visitor Acceptable Use Agreement
- Parent/Carer acknowledgement of AUA (signed as part of the home/school agreement)
- Record of monitoring concerns/devices/internet sites (responding to incidents of misuse) - this is done via My Concern and the monitoring system in place at the time
- Reporting Log - data from My Concern
- Training Needs Audit Log

Pupil Acceptable Use Policy Agreement - (EYFS / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet
- If I have to use a computer at home to do my learning I will use it safely just as my teacher tells me to
- If I have to use a computer at home to do my learning I will be respectful of other children in the online classroom and use kind words only

Signed (children of class …

Date:

Acceptable Use Agreement –KS2

- I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

  For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will never arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that everyone has equal rights to use technology as a resource and:
- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).
- I will act as I expect others to act toward me: I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission.
- I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites.
- When using the internet for research or recreation, I recognise that: I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that I am responsible for my actions, both in and out of school:
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I will use Google Classroom respectfully and safely (both in school and at home) and follow the rules that my teacher has set to ensure that I am using it correctly.
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action.
- This may include loss of access to the school network / internet, suspensions, contact with parents and in the event of illegal activities involving the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

Pupil Acceptable Use Agreement - (KS2)

Please sign below to show that you have read, understood and agree to the statements included in the Acceptable Use Agreement.

If you do not sign this agreement, access will not be granted to school systems.

I have read and understand the KS2 Pupil Acceptable Use Agreement and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing the online classrooms, school programs, websites etc.
- I use Google Classroom (both in and out of school).

Signed:

Name of Pupil:

Date: