The Academy at St James
Chelwood Drive Bradford
BD15 7YD
Telephone: 01274 777095
Head of School: Mr Chris Tolson

E-SAFETY AND ACCEPTABLE USE POLICY

Reviewed and Approved by: - Liz Lawley

Date - 2.7.20

Signature:- R Smith (Computing Lead) C Tolson (Headteacher)

Next Review date- 2.7.21

The Academy at St. James

E-Safety / Internet Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

The purpose of Internet access in schools is to raise educational standards, enhance and extend pupils' education, to support the professional work of staff and to enhance the school's management information, and business administration systems.

Access to the Internet is a necessary tool for staff and an entitlement for students who show a responsible and mature approach. It should be noted that the use of computer systems without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

However, the use of these new technologies can put young people at risk both at home and at school. Some of these risks include:

- Gaining access to illegal, harmful or inappropriate content/ images
- Inappropriate communication with others- including strangers
- Sharing personal information
- Online bullying
- Gaining access to unsuitable videos/ games/
- Plagiarism and copyright infringement
- The risk of being groomed
- Sharing personal images without an individual's consent or knowledge
- Illegal downloading
- Potential for excessive use which may impact upon the social and emotional development and learning of the young person
- Not having the necessary skills to evaluate the quality, accuracy and relevance of information that young people can access online

As with all of these risks, it is impossible to eliminate these risks completely. It is therefore imperative that here at The Academy at St James we embed a thorough educational provision in order to help keep our children safe. We will do this by building pupils' awareness of the risks that they may be exposed to and provide them with the confidence, skills and understanding which they will require in order to seek advice and deal with any risk that they encounter in an appropriate manner.

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported Online Safety incidents
- Monitoring of network activity
- Pupil Online Safeguarding survey data which is gathered through annual questionnaires
- Evaluation of children's work
- Pupil discussions at school council
- Monitoring evidence of work through digital portfolio

Roles and responsibilities:

Everyone plays a role in ensuring that our children are kept safe when having access to all areas of technology both within their homes and when at school.

Governors

Governors are responsible for the approval of the Online Safeguarding policy and for reviewing the effectiveness of the policy. The Governor responsible for Online Safeguarding is John Watts

The role of the Governors will include:

- Monitoring online safety incidents
- Reporting/Updating the Governing body at Governors meetings

Head Teacher and SLT

The role of the Head and Leadership team includes:

- The Head Teacher is responsible for ensuring the safety (including online safety) of members of the school community
- Ensuring that all staff have suitable CPD to enable them to carry out their duties to the highest of standards.
- Being aware of the procedures that must be followed in the event of a serious online safety allegation being made against a member of staff. This is detailed within the child protection policy.
- Being aware of 'Actions upon discovering inappropriate or illegal material' guidance from Bradford Curriculum ICT Team.

Online Safety Coordinator (s)

It is the role of the Online Safety Coordinator/ Safeguarding lead to ensure that all staff are aware of the policies and procedures that must be followed in the event of an online safety incident taking place. They will respond to any incidents that they have received and report on them further if required. They will ensure that all incidents are dealt with in correspondence to school policy and that the information is shared on a need to know basis when appropriate.

Technician

Primary Technology provide our technical support.
The school technician ensures:

- That the school's ICT infrastructures are secure and not open to misuse or malicious attack.
- That monitoring software, filtering systems, Wi-Fi networks and antivirus software are implemented and updated as required.

Teaching and support staff

All members of staff in school will keep up to date on online safety matters through CPD provided. They must all ensure that they understand the process of reporting online safety incidents which must be done immediately. It is also the role of the staff to ensure that opportunities for children to learn about online safety issues are embedded across all areas of the curriculum in addition to the discrete online safety lesson which must be planned and taught every half term. Staff are also responsible in ensuring that pupils understand and follow the user agreement that they have signed.

Designated Safeguarding lead for Child Protection

The named person responsible for child protection is trained in online safety issues and is aware of the potential for serious child protection issues that may arise from:

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

Pupils

Pupils are responsible for using the school ICT systems and equipment in accordance with the Pupil Acceptable Use Policy. Pupils are provided with strategies to use when they are exposed to risks and are encouraged to share any online safety concerns that they have with a trusted adult.

Parents/Carers

At the Academy at St James we take every opportunity to help parents/carers to understand online safety issues. We will raise awareness of the key issues in the following ways:

- Parent/Carer information sessions on Online Safety
- Parents are asked to discuss Acceptable use policies with their child and are invited to contact school if they would like to discuss matters further
- Information about Online Safety (and related policies) are available on the school website
- Key information is also shared via letters and newsletters
- Specific support for individual families where there is a greater risk

Community user's/School visitors

All visitors to school are required to agree to our Visitor Acceptable Use Agreement. A copy of this is available to them when they sign in.

Pupil Education

Here at The Academy at St James we understand how crucial it is for our children to be able to identify the dangers that they may be exposed to in order for them to be able to recognise these dangers effectively when working independently. This will not only support our children to build their awareness enabling them to avoid some of the risks that they face online; but also provide them with the strategies that they can put into place when they have been exposed to a potential risk.

Online safety education will be provided in the following ways:

- A planned Online Safety programme is delivered through ICT and PSHE in the form of the TIC Bradford scheme.
- This scheme also highlights Online Safeguarding issues that arise in the context of ICT lessons.
- Pupils are taught in all lessons to be aware of the content that they access online and learn how to validate the accuracy of the information they find.
- Rules for acceptable use are shared at the beginning of each academic year and with any new starters as they join school.
- Pupils are taught how to search for information safely and safe search engines are used by Teaching Staff.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Copyright free images and audio sources are shared with the children and are included in the Bradford ICT Scheme of work.
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children.
- Pupils know that any events of online bullying are taken seriously by the school and they understand the importance of sharing their concerns with a trusted adult.

Staff Education

At The Academy at St James we also recognise that it is essential that all of our staff receive regular Online Safeguarding training in order for them to have the necessary skills and knowledge which is ultimately required for keeping our children safe.

Training will be offered as follows:

- Annual Online Safety staff training to be delivered to all staff by West Yorkshire Police Bradford District Cyber Team
- An annual survey of staff Online Safety training will be completed and any training needs identified.
- The annual questionnaire results from Parents and Pupils will highlight issues relevant to the school and particular year groups. These will be used to direct training.
- Monitoring the teaching of online safety regularly and further training needs identified.
- Staff have access to all policies on the T Drive

Governor Education

Governors are invited to take part in annual Online Safeguarding training sessions with staff.

Internet Provision

The school internet is provided by Bradford Learning Network. All sites are filtered using Smoothwall' web-filtering software, which generates reports on user activity. If staff require access to a site that is blocked, they must firstly contact SLT for approval. Once approval is given the site can be accessed.

Managing ICT systems and access

Access to ICT systems is managed by the Technician and Computing Coordinator (Rebecca Smith). Every child has their own login for the laptops and chrome books which includes a username and a password. Children also have access to relevant accounts such as TTRockstars, Education City, Scratch pad etc. These accounts are managed through administrator privileges which are only known to the Technician and Computing Coordinator. Accounts are created for new starters at the beginning of the academic year and then for new starters that join during the school year. Accounts are deleted annually for any leavers including those children in year 6.

Passwords

All users regardless if they are staff or pupils have the responsibility for ensuring the security of their username and password and must not allow others to have access to their log on details (as per Acceptable Use Policies). Any concerns about sharing passwords or log on details must be reported to the Online Safety Coordinator or a member of SLT immediately. All staff members accounts must have a password. New staff are made aware of the school's password rules through induction, the Acceptable Use Policy and the Online Safeguarding policy. These policies are accessible at all times for staff to refer back to. Pupils have an individual log on that must be used whenever they access the school's ICT systems. They are made aware of the dangers of sharing their passwords and other personal information through the discrete teaching of ICT/Online safety lessons and through the Pupil Acceptable User Policy. Passwords for new users and replacement passwords for existing users are allocated through our Primary Technology Technician who is in school for 2 half days per week.

The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the *Head teacher* or other nominated senior leader and kept in a secure place e.g. school safe.

Filtering

The Academy at St James uses 'Smoothwall' web' filtering software to prevent people from accessing potentially undesirable and objectionable material on the internet. This software sits on the broadband network and monitors requests for web pages and intercepting requests for sites that have been blocked. Sites can be added to and removed from the database after approval by a member of SLT by an administrator.

In order to minimise the risk of our pupils being exposed to risks online and in order to keep up with ever changing technologies, new sites and apps; the list of banned sited is updated regularly by Smoothwall administrators. In addition to this, teachers are encouraged to report all sites which they deem as inappropriate (and which can still be accessed) to the ICT Co-ordinator which will then have the site blocked for our school.

Personal Data Protection

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

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

All staff must ensure:

- Personal data is kept safe at all times to minimise the risk of it loss or further use
- Personal data is only accessed on computers or other devices that have a secure password. They must also ensure that they are 'logged off' at the end of every session
- That all USB/ memory sticks are password protected

Use of digital and video images (photographic and video)

Staff are allowed to take digital/video images of the children to support educational aims. These images should **only** be taken on school equipment. Every teacher has a teacher iPad that can be used for this. Parental permission is sought for every child in school regarding how photographs can be used or shared (School website/ Twitter). Permission slips are stored securely in their individual files and records of permission are shared with each class teacher. Teaching staff are responsible for storing photographs and images safely and securely. Digital leaders are also going to play a role in ensuring the iPads have photos regularly deleted.

Management of assets

All ICT assets are recorded on an inventory spreadsheet by our Primary Technology Technician. Assets that are damaged or surplus to requirements have data removed by the Technician before being collected and destroyed by a reputable company. Certificates are received and filed where this has taken place.

Responding to incidents of misuse

Although we hope that all members of our school community will be responsible ICT Users and abide by their Acceptable User Agreement; this however may not always be the case and we need to ensure that we have appropriate measures in place in order to respond to these incidents in the most effective way.

In the event of misuse taking place which appears to involve illegal activity such as:

- Child sexual abuse images
- Adult material which breaches the Obscene Publications Act
- Criminally racist material, including evidence of Radicalisation or a breach of Prevent
- Other criminal conduct, activity or materials

it is important that the device is not shut down as evidence could be erased but that it is removed to secure location. All matters should be reported immediately to the Head/Online Safety Coordinator.

Misuse that has taken place that is not illegal will be dealt with using the sanctions listed below/ through the school behaviour policy. These incidents must be recorded on CPOMs and parents must be informed when appropriate..

Cyberbullying

Cyberbullying can be defined as the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Pupils are taught about cyberbullying through Online Safety and PSHE lessons. During this time, pupils are given advice on how to respond to cyberbullying – not to forward messages to other people and not to reply. Instead all pupils are encouraged to share any concerns of cyberbullying with a trusted adult. Staff will support children who are victims of cyberbullying by supporting them to collect evidence of the bullying that has taken place. Ideally this would include time, date and a screen capture.

Full details of how the school manages incidences of bullying can be found in our Anti-Bullying policy. Serious incidents of bullying may be reported to the Police.

Social Media

At The Academy at St James we use Social Media in the following ways:

- Twitter
- Facebook
- Pobble
-

It is imperative that all members of staff keep their personal and professional lives separate on social media.

Mobile devices

Personal mobile devices must not be used around school. Staff are able to have access to their mobile phones in the staff room which has a locked door. Pupils turn off their mobile phones and hand them in at the office where they are safely stored until collection after school. School do have a number of school mobiles that can be used following the Acceptable Use Agreement.

Rules for Internet Access

The school has developed a set of guidelines for Internet use by pupils. These rules will be made available to all, and kept under constant review. All members of staff are responsible for explaining the rules and their implications, and need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

- Pupils should only access the Internet for study purposes or for school authorised/ supervised activities
- Pupils must ask permission to use the Internet in lessons and should not print pages from it unless authorised to do so.
- Pupils must not use the Internet to obtain, send, print or display messages or pictures that are unlawful, obscene or abusive
- Pupils must respect the work and ownership rights of others and should always try to abide by copyright law
- Pupils should never give personal information to those who they contact through any electronic communication
- Pupils should never use an image of another child or adult without their consent and should understand how cyber-bullying, in all its forms, is unacceptable
- Pupils should take care when using any computers, software and other ICT hardware to avoid damaging them. Where equipment has been damaged, it should be reported to the class teacher immediately
- Pupils should keep their usernames and passwords for the network and any online resources safe
- Pupils must not attempt to use usernames and passwords that belong to others, nor should they use their folders, work or files
- Pupils should immediately report anything that they see, which they think is unpleasant or unsuitable

These rules will be simplified so that children understand clearly what is acceptable and displayed in the classroom. Children will be expected to sign the rules to show they understand and agree to them. (See e-safety rules for KS1 and KS2 in appendix)

Sanctions

Should any of the rules be broken, then the following sanctions will be used:

- Temporary or permanent ban on Internet use
- Letters may be sent home to parents/carers
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- In extreme cases legal action may be taken or the police and local authorities may be involved.

How will E-mail and other online communication be managed?

Pupils will, on occasion, be allowed to use email or other online communication methods to contact other people.

- Teachers will be responsible for ensuring that pupils are aware that the content of emails, like any other correspondence, is appropriate and suitable for sharing, and will supervise this appropriately.
- When required, pupils can be given an e-mail address, which they can use with supervision and instruction from the class teacher. Each pupil's inbox will be accessible by the ICT Co-ordinator and Senior Leadership Team.
- The email system automatically monitors for profanities and inappropriate sexual language. Any abuse will be reported to the ICT Co-ordinator who will take action in line with this policy.

About the policy:

The Acceptable Use Policy was written by the ICT Co-ordinator in conjunction with the leadership team. It will be reviewed on a yearly basis and ratified by the ICT governor.

Appendices

- Letter from Head Teacher to parents.
- KS1 e-safetyrules
- KS2 e-safetyrules
- Child & Parent / Carer Acceptable Use Agreement.
- Staff / Volunteer - Acceptable Use Policy Agreement

The Academy at St. James
Chelwood Drive, Bradford
BD15 7YD
Telephone: 01274 777095

Dear Parent/Guardian

Responsible Use of the Internet in School

As part of the school's ICT curriculum we offer pupils supervised access to the Internet. Before being allowed to use the Internet, all pupils must obtain parental permission and parents/guardians must sign the permission slip as evidence of your approval and their acceptance of the school rules on this matter.

On occasion, pupils will be able to exchange electronic mail with children in other schools and research information from museums, libraries, news providers and suitable websites as part of their learning.

Our aim for Internet use is to further educational goals and objectives. Pupils benefit from access to the Internet, in the form of information resources and opportunities for collaboration.

Ultimately, parents and guardians are responsible for setting and conveying the standards that their children should follow when using media and information sources. During school, teachers will guide pupils towards appropriate materials. Outside of school, families bear the same responsibility for such guidance as they access information sources such as television, telephones, movies, radio and other potentially offensive media. Please take a look at our school website where we have a list of extremely useful resources aimed at ensuring our children are safe when online.

In addition, we may publish children's work and photographs (with no name attached) of activities/events in school on the Internet through the school's own website.

Please read and discuss the attached Internet Safety Rules with your child and then sign the slip giving permission for your child/children to use the internet and have their photographs (where required) published on the school's website.

Yours sincerely,
Mr C Tolson
Head of School

"ASPIRE, ACHIEVE, BELIEVE"

Key Stage 1

Think then Click

e-Safety Rules for Key Stage 1 - These rules help us to stay safe on the Internet

- We only use computers or iPads when an adult asks us to.
- We click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask for help if something goes wrong.
- We will always try to look after all school ICT equipment.

We would like our parents and carers to help us stay safe on the internet by:

- Getting to know and regularly talking with us about the things we are using the internet for, both at home and in school.
- Learning with us about how to use the internet safely and responsibly
- Making use of the Internet part of our family activity, working with us as we learn how to use the Internet in a safe, responsible and respectful way
  Setting clear ground rules, expectations and guidelines for how we should use ICT, mobile phones, electronic devices and games consoles which connect to the internet at home and in school.
- Reminding us of and discussing these rules, displaying them near the computer as a reminder to both of us, of the way we should behave when we use the internet.
- Monitoring the amount of time we spend using ICT, mobile phones, electronic devices and games consoles which connect to the internet
- Being aware to whom we are talking both on our phone and online ~ including social network sites

Key Stage 2

Think then Click
e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- If we send e-mails or other online communications, we ensure that they are polite and friendly and we only contact people an adult has approved.
- We do not open e-mails sent by anyone we don't know.
- We never give out personal information.
- We never arrange to meet anyone we don't know.
- We do not share our passwords with anyone.
- We do not download or save files to our computer without permission.
- We always acknowledge and thank other people if we use their work, by telling others where it came from.
- We ask and get permission before we take or use photographs of our friends in emails, in electronic publications or on any websites.
- We understand the harm that cyber-bullying can cause and we work together to stop it happening.
- We understand that if we do not follow these rules then our parents will be informed and we may not be allowed to use the internet in school.

We would like our parents and carers to help us stay safe on the internet by:

- Getting to know and regularly talking with us about the things we are using the internet for, both at home and in school.
- Learning with us about how to use the internet safely and responsibly
- Making use of the Internet part of our family activity, working with us as we learn how to use the Internet in a safe, responsible and respectful way
- Setting clear ground rules, expectations and guidelines for how we should use ICT, mobile phones, electronic devices and games consoles which connect to the internet at home and in school.
- Reminding us of and discussing these rules, displaying them near the computer as a reminder to both of us, of the way we should behave when we use the internet.
- Monitoring the amount of time we spend using ICT, mobile phones, electronic devices and games consoles which connect to the internet
- Being aware to whom we are talking both on our phone and online ~ including social network sites

Parent / Carer Acceptable Use Agreement

All pupils are entitled to use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.
Pupil:
Class:

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.

Signed:

Date:

Parent's/ Carers Consent for Web Publication of Work and Children's Photographs and Parent's Carer's Consent for Internet Access

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital devices to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images of your child may be recorded during school activities and used to celebrate success through their publication in newsletters, on the school website, local newspapers or other carefully selected educational websites e.g. Lend me your Literacy.

Parents / Carers who do not wish their child's photographs to be published online or in the newsletter should inform the school in writing.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed:

Date:

Please print name:

Please complete, sign and return to the school office

Staff / Volunteer - Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I will not disclose my username or password to anyone else, 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission only. I will not use my personal equipment to record these images. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (schools / academies should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (Where staff / volunteers are 'friends' with parents of children within school, online communication which can be viewed by others (eg Facebook, Twitter etc) should not mention the school by name or disclose any details about the professional life of the school.
- I will not engage in any on-line activity that may compromise my professional responsibilities or which may bring the good name of the school into disrepute.

- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
  - I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , 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 try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer. All new software installation should be completed by the ICT technician.
• I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
• Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
• I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
• I will immediately report any damage or faults involving equipment or software, however this may have happened.

I understand that I am responsible for my actions in and out of the school:

• I understand that this Acceptable Use Policy applies not only to my work and use of school / academy ICT equipment in school, but also applies to my use of school / academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools / academies should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

The Academy at St. James – E-Safety / Internet Acceptable Use Policy

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

This Acceptable Use Policy is intended to ensure:

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- The school will try to ensure that pupils have good access to ICT to enhance their learning opportunities and will, in return, expect pupils to agree to be responsible users.

Staff / Volunteers:

- that staff / Volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff / Volunteers are protected from potential risk in their use of ICT in their everyday work
- The school will try to ensure that staff have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff to agree to be responsible users

How will risks be assessed?

In common with other information resources such as magazines, books, television and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate materials.