Clayton Village Primary School
E-safety policy 2018

1. Scope of the Policy

This policy applies to all members of, and visitors to, the school (including staff, pupils, volunteers, parents/carers, and any visitors to the school site.) The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other eSafeguarding incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The school will deal with such incidents and associated behaviour detailed in this policy and linked policies (e.g. antibullying policy) and will, where known, inform parents/carers of incidents of inappropriate Online safety behaviour that take place out of school.

2. 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 school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

- Through a planned Online safety curriculum reinforced through a programme of assemblies and pastoral activities (e.g. Safer Internet Day).
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- They are taught to acknowledge the source of information they use and to respect copyright when using material accessed on the internet.
- Pupils are helped to understand the need for the 'Pupil Acceptable Use Agreement' and encouraged to adopt safe and responsible use both within and outside school.
- Staff 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 are guided to sites checked as suitable for their use.
- 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 are vigilant in monitoring the content of the websites the young people visit and encourage children to use child friendly search engines.
- To augment the scheme of work, a local PCSO delivers sessions to our children in Key Stage 2, which include advice about the legal implications of negative online behaviours and how to access the help available from the police.
- Curriculum Resources and suggested activities from relevant organisations (e.g., NSPCC, Childnet) are researched and added to the long-term plan to ensure that our school's response to the continuous developments in this sphere is up to date and relevant.
- Teachers will monitor children's use of iPads through the classroom app.

Education- Parents

Many 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 may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site, text message links
- Parents / Carers sessions
- High profile events / campaigns e.g. Safer Internet Day

Education- Staff

- A planned programme of formal online safety training will be undertaken by staff. This will be regularly updated and reinforced. An audit of the eSafeguarding training needs of all staff is carried out regularly.
- All new staff and volunteers receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The Online Safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The reviewed eSafeguarding policy and updates will be presented to and discussed by staff in staff/team meetings when relevant.
- The eSafeguarding Coordinator will provide advice/guidance/training to individuals and groups as required.

3. 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 eSafeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors on receiving regular information about eSafeguarding incidents and monitoring reports from the eSafeguarding Governor. eSafeguarding is a regular agenda item for Governors.

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for eSafeguarding will be delegated to the Online Safety Officer.
- 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 eSafeguarding allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Online Safety Officer and other staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues, as relevant.
- The Headteacher will ensure that CPOMs is used 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 to those colleagues who take on important monitoring roles.
- The Senior Leadership Team and Safeguarding Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

- Is a member of the Safeguarding team where current issues are discussed and incidents reviewed
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school 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 through CPOMs
- Reports regularly to the Safeguarding Team and SLT

Technical Staff

Are responsible for ensuring that:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that they are up to date with e-safety technical information and updates the E Safeguarding leader as relevant
- that monitoring software (e-safe) and anti-virus software is implemented and updated

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safeguarding leader for investigation through CPOMs
- digital communications with students / pupils (email/website /voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Designated Safeguarding Lead:

The DSL is trained in eSafeguarding issues and so is aware of the potential for serious child protection/safeguarding issues that 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

They are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy (Y1 onwards)

They should:

- develop a good understanding of the need to avoid plagiarism and uphold copyright regulations and use good internet research skills
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand policies on the use of mobile devices and digital cameras
- know and understand policies on the taking/use of images and on cyber-bullying
- understand the importance of adopting good on-line safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school.

They are aware of these sanctions for misuse of digital technologies in school: -

  - Acknowledge misuse/misconduct when actions discussed with Online Safety Officer/class teacher
  - Repeated or serious misuse/misconduct will result in restricted use of IT equipment for set period and requirement for learning tasks to be completed without IT resources (as set out in Appendix 5)
  - Serious or continued misuse/misconduct will be brought to the attention of the Headteacher and parents of the pupil

Safeguarding Group

The Safeguarding Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

Members of the group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school online safety policy / documents
- the production / review / monitoring of the school filtering policy and requests for filtering changes
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

4. Technical infrastructure/ equipment/ filtering and monitoring

The school will be responsible for ensuring that the school 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:

- There will be regular reviews and audits of the safety and security of school technical systems
- 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 at Key Stage 2 and above will be provided with a username and secure password by LDD. All users in Key Stage 1 will have individual usernames with a class specific password.
- The ICT manager 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.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Internet filter systems will be checked termly by a member of the safeguarding team.
- E-safe is used in school. This is a monitoring system which will track images and websites searched by staff and children as well as key logging anything typed on a school device (laptop or PC).
- E-safe produces weekly update reports where any incidents are reported to the Headteacher (staff) and E safety officer (children).
- In the case of incident where a child is at immediate risk or suspicious activity reported, the Headteacher will be immediately contacted.
- 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 school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

5. Mobile Technologies

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.
All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils and guests 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 device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*			
Internet only					*Yes*	*Yes*
No network or internet access				*Yes*		

Staff- school devices

- Staff are provided with a laptop and ipad which is for school use and can be used throughout the school day and in all areas of the school
- These devices will be given access to the school network and internet
- These devices will be filtered and monitored through school systems
- Staff may download and install their own apps to the ipads but these should be for educational purposes
- Staff laptops should be encrypted
- Staff ipads should be locked with an alphanumeric password which will provide a higher level of security
- If a staff member leaves employment, they should return the ipad wiped and reset to factory settings.
- If a staff member damages their device, they are liable for the charges for repair.

Personal devices

- Staff and guests are allowed mobile devices in school
- Children are not allowed mobile devices in school. If a child does bring their device, it must be kept locked away either by the class teacher or in the office.
- Staff and guests must not use their personal devices in front of children.
- Mobile devices are a vital part of the school's lockdown procedure; where staff may use them to communicate with each other regarding the safety of the children.
- Personal laptops may be given internet access but they will not be able to access the network.
- Personal phones will not be given internet access.
- No technical support is available for personal devices.
- Children's personal data should not be stored on personal devices and it is strongly recommended that staff use school provided devices.
- Taking / storage / use of images on personal devices is not allowed.
- Children will be educated regarding the safe use of mobile devices as part of the online safety curriculum.

6. Use of digital video/images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or

embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press see appendix 3
- 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). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers. This is gained through the agreement in appendix 3

7. Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018. Further information on this is in the Data Protection policy.
The school will ensure that:

- Data stored on portable electronic devices are encrypted
- Any loss of portable devices with data is reported, as appropriate, to the ICO.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Staff will not share their passwords to ensure data is kept secure.
- Printer systems are password protected so that any personal data printed is secure.

8. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official *school* email service may be regarded as safe and secure.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs etc) must be professional in tone and content. These communications may only take place on official school 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 school website and only official email addresses should be used to identify members of staff.

Appendices

1. Acceptable use policy- staff
2. Acceptable use policy- children
3. Consent form- including video/ photo permission (parents)
4. Acceptable use agreement- guests
5. Actions and sanctions
6. Incident flowchart

Appendix 1

Staff Acceptable Use Policy

School 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.

This Acceptable Use Policy is intended to ensure:

- that staff and 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 are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

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 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 will 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, iPad) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the 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 ensure that my devices are locked when they are not in use.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- My school email address will be my principal method of online communication.

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 and in accordance with the school's policy on the use of digital / video images.
- I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website/ twitter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will report any inappropriate activity seen by myself or a pupil using CPOMS, and tag in the E-safety officer.

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:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted (using the provided memory stick).
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity:

- I will 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 download or distribute copies (including music and videos).

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 ICT equipment in school, but also applies to my use of school 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 .
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

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	

Appendix 2

Key Stage One
Pupil Acceptable Use Policy.

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
- I will only use activities that a teacher or suitable adult has told or 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 will not delete it; I will show the adult.
- I know that if I break the rules I might not be allowed to use a computer.
- The school will monitor how I use a computer to check I am being safe

---

All pupils have access to computers and the internet as an essential part of learning, as required by the National Curriculum. Both pupils and parents are asked to sign below to show that the e-safety rules have been understood and agreed

Name of pupil: _____

Pupil's Agreement

- I have read and I understand the school e-safety rules
- I will use the computer and Internet in a responsible way at all times
- I know that Internet access may be monitored

Parental Agreement

I have read and understood the school e-safety rules and agree that my son/daughter will access the internet following these rules. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate material.

Signed: _____ Date: _____

Key Stage Two
Pupil Acceptable Use Policy.

- I will only use ICT equipment for purposes agreed with a member of staff
- I will ask permission before entering any website, unless my teacher has already approved that site
- 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 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 only email people I know, or my teacher has approved
- I will be polite and responsible when I communicate with others online as I should in real life
- I will not create or send material which is deliberately intended to cause upset to other people
- I will not disclose or share personal information about myself or others when on-line
- I will not use internet chat
- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to a trusted adult. I will save it and not delete it.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be sanctioned, it may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.
- 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

---

All pupils have access to computers and the internet as an essential part of learning, as required by the National Curriculum. Both pupils and parents are asked to sign below to show that the e-safety rules have been understood and agreed

Pupil's Agreement

- I have read and I understand the school e-safety rules
- I will use the computer and Internet in a responsible way at all times
- I know that Internet access may be monitored

Signed by pupil: _____

Parental Agreement

I have read and understood the school e-safety rules and agree that my son/daughter will access the internet following these rules. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate material.

Signed: _____ Date: _____

Appendix 3

Consent Form

Child's Name ……

Child's Class……

Throughout the year we aim to provide a variety of opportunities to enhance your child's education. These opportunities will include walks within the local community, tasting different foods, taking photographs and filming our achievements. Suitable risk assessments will be carried out prior to any activity and all activities will be supervised accordingly. Please indicate below if you are happy for your child to take part with the following activities. This consent form will cover the whole time your child is with us. If at any point you change your mind, we will need to know in writing about any changes which need to be made.

Local Area and Walks

I give/do not give permission for my Child to take part in local walks within a 3 mile radius of the school.

Signed …… (Parents / Carer)

Food

I give/do not give permission for my child to take part in food tasting or cooking activities.

Any known allergies ……
Your child may still take part in these activities but will not be exposed to these foods.

Signed …….. (Parents / Carer)

Photographs and Video Recordings

I give permission for my child to be photographed and filmed and for these recordings to be used only within the school community. Permission for this would also include performances, assemblies and everyday classroom learning. As part of the ICT curriculum all children are taught and participate in digital imagery.

Signed …… (Parents / Carer)

I agree that if, with the permission of the Headteacher*, I take photographs or videos of any school event, I will ensure that these are used for personal and family use only, and will not be made available to anyone else. I understand that any other use may be in breach of the Data Protection Act 1998.

Signed …… (Parents / Carer)

** The Headteacher or Deputy Head Teacher will inform parents/carers if events can be filmed or photographed.*

Publishing of Pupil Photographs and Pupil Work

I give permission to publish my child's **photo/work** (please delete as appropriate) in general media appearances (local/national media/press releases sent to the press highlighting a school activity) or on the school website and blog. Pupil's full names will not be used anywhere on the website, particularly in association with photographs.

Signed …… (Parents / Carer)

Appendix 4

Acceptable Use Agreement for Guests

By signing into our school you agree to follow our safeguarding and child protection policies, including Online Safety:

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use personal devices that I've brought into school for activity's that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher (Miss Cradock) or ESafety Lead (Miss Clifton).
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will 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 download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

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 and by signing into school agreed to adhere to these procedures.

Guest Wifi login:
Guest PC login:

Appendix 5

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

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

Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to ICT manager	Refer to SLT/ Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone / digital camera / other mobile device	X							X	
Unauthorised downloading or uploading of files		X			X			X	
Attempting to access or accessing the school network, using another student's / pupil's account		X				X	X		
Attempting to access or accessing the school / 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	X		X
Continued infringements of the above, following previous warnings or sanctions			X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X	X		X
Using proxy sites or other means to subvert the school's / academy's filtering system		X			X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X			X	
Deliberately accessing or trying to access offensive or pornographic material			X		X	X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X			X			X	