Learning together to be
the best we can be

Headteacher - Nichola Irving

HORTON
GRANGE
PRIMARY
SCHOOL

Online Safety Policy

Safeguarding Statement

Everyone at Horton Grange shares an objective to help keep children and young people safe by contributing to:

- Providing a safe environment for children and young people to learn in school and;
- Identifying children and young people who are suffering or likely to suffer significant harm, and taking appropriate action with the aim of making sure they are kept safe both at home and in school.

DATE ADOPTED: FEBRUARY 2020

Headteacher – Nichola Irving
Online Safety Co-ordinator – Hamish Fields
Deputy Online Safety Co-ordinator – Emma Brownrigg
Online Safety Governor – Karl Lunn
Chair of Governors – Janet Dyson
Safeguarding Governor – Peter Standfield
ICT Technician – John Harwood
Computing Subject Leader – Hamish Fields

Online safety encompasses the use of new and existing technologies, internet and electronic communications such as mobile phones, IPADs, collaboration tools and personal publishing.

The school's Online Safety Policy will operate in conjunction with other policies

- ➢ Behaviour
- ➢ Anti-bullying
- ➢ Child protection
- ➢ Curriculum
- ➢ Data Protection
- ➢ Photography
- ➢ Preventing extremism and radicalisation
- ➢ Social networking policy and guidance
- ➢ IT Security Policy
- ➢ Staff Code of Conduct

Online safety relies on effective practice at a number of levels:

- Responsible ICT use by all staff and students encouraged by education and made explicit through published policies;
- Sound implementation of Online Safety Policy in both administration and curriculum, including secure school network design and use;
- Safe and secure broadband including the effective management of filtering;
- The appointment of an Online Safety Co-ordinator and deputy to implement and manage this policy;
- The support of the headteacher and governing body;
- Supporting parents in the use of ICT and emerging technologies at home, including advice on gaming and parental settings for devices .

1. Introduction

The purpose of this policy is to:

- Establish ground rules that are in place in Horton Grange Primary School for using the internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate the pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience and make the most of the vast and varied online world in a safe way.
- Describe how these fit into the wider context of our discipline and PSHE policies;
- Demonstrate the methods used to protect children from accessing sites containing inappropriate material such as pornography, racist or politically extreme views and violence;
- To be reviewed regularly and in the light of new technologies. This will be carried out with the involvement of staff, pupils, governors and parents.

Roles and Responsibilities

Governors

Governors are responsible for approving the Online Safety Policy and reviewing its effectiveness on an annual basis. Governors will be updated of online safety incidents as appropriate. A member of the governing body has been designated as the Online Safety Governor.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher is responsible for ensuring that that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their roles as necessary.
- The Headteacher will ensure that there is a system in place for monitoring and support of those in school who carry out the internal online safety role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles e.g. weekly SENSO reports.

Online Safety Co-ordinator

- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing school online safety policies.
- Are responsible for regularly monitoring internet and device use via SENSO and updates the headteacher, governors and senior managers on a regular basis.
- Acts as a point of contact for online safety issues within the school.
- Supports the national online safety strategy and disseminates up to date information among the staff and arranges staff development as a result of information regarding emerging and changing technologies.
- Is also jointly responsible along with the Designated Person for Child Protection and Safeguarding Co-ordinator for the duty of care requirements under the Safeguarding arrangement within school.
- Is supported in this role by the Deputy Online Safety Co-ordinator.
- Liaises with LA and the school technician.
- Provides training and advice to staff.
- Liaises with staff to help deliver work during Internet Safety Week each year as well as supporting the delivery of online safety through the curriculum

ICT Technician is responsible for ensuring:

- the school’s technical infrastructure is secure and not open to misuse or malicious attack.
- the school meets required online safety technical requirements and any LA 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/VLE/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher for investigation.
- that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy Agreement (AUP).
- they report any suspected misuse or problem to the Headteacher for investigation.
- all digital communications with children/parents/carers should be on a professional level.
- online safety is embedded in all aspects of the curriculum.
- children understand and follow the online safety and AUP.
- 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, camera etc in lessons and other school activities (where permitted) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned, children should be guided to sites checked as suitable for their use and procedures are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection/Safeguarding Designated Leads should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing or personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil AUP
- are developing 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 (switch off monitor ONLY and report to a member of staff immediately).
- will be expected to know and understand policies on the use of mobile devices and digital cameras
- should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use both within and outside school
- should know and understand policies on the taking/use of images and on cyber-bullying
- should understand the importance of adopting good online safety practices when using digital technologies out of school and realise that the Online Safety Policy covers their actions out of school, if related to their membership of the school

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 school will take every opportunity to help parents understand these issues through workshops, newsletters, parents' evenings, letters, website, weekly online safety updates, information about local and national online safety campaigns and relevant literature. Parents and carers will be encouraged to support the school in promoting good online safety practices and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/VLE and online pupil records

2. Teaching and Learning

Although regulations and technical solutions are important, there must be a balance with educating children to take a responsible approach. Therefore, education of online safety is an essential component 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.

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 / PSHE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and class 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 helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

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 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, website,
- Parents / Carers sessions
- High profile events / campaigns eg Safer Internet Day
- Regular online safety updates uploaded onto the school's Facebook Page
- Reference to the relevant web sites / publications eg http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

- Online Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online information for the wider community
- Supporting community groups eg Early Years Settings, to enhance their online safety provision
- Providing family learning courses in the use of new digital technologies, digital literacy and online safety

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:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should 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 Co-ordinator will receive regular updates through attendance at external training events (eg 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 meetings.
- The Online Safety Co-ordinator 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 sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents where possible

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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:

- School 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 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 (in KS1 and 2) will be provided with a username and secure password by the IT technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The "master / administrator" passwords for the school ICT system, used by the IT technician must also be available to the Headteacher or other nominated senior leader and kept in a secure place

- IT Technician 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
- Technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, 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 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" onto the school systems
- An agreed policy is in place (see Acceptable Use) regarding the extent of personal use that users and their family members are allowed on school devices that may be used outside of school.
- It is agrees that staff are using their professional judgement/experiences, allowed to download executable files and install programmes on school devices.
- 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. All staff are encouraged to use the cloud storage provided.

3. Using Technologies

- The school's curriculum ICT system is monitored by SENSO which sends weekly updates to the Online Safety Co-ordinator regarding unacceptable use of the system. This identifies individual pupils, staff or computers which have been used and reports on the types of inappropriate access. This can then be managed according to the school's behaviour policy.
- Mobile devices (IPADs) have Lightspeed recommended firewalls installed on them which are regularly updated if the internet is accessible on the devices. This monitors all internet activity.
- Virus protection is updated regularly by the ICT Technician.
- Staff are not permitted to access the school's wireless technology with their personal laptops unless SENSO is installed.
- Staff using school laptops at home are aware that PCE is installed on all units and that the appropriate use of the equipment will be monitored when the laptop accesses the school's wireless system on its return to school.

E-Mail

- Pupils may only use approved email accounts on the school system where available (eg School 360).
- Pupils must immediately tell a teacher if they receive offensive material or comments via email.
- Pupils are taught not to reveal personal details of themselves or others in electronic communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper
- Staff should, wherever possible, use the admin email address for contacting parents. Personal or NCC email addresses should not be used to contact parents without discussing the

implications of this with the Online Safety Co-ordinator/ headteacher. If parents make contact through the county email system, this should be reported to the Online Safety Co-ordinator.

- Under no circumstances should staff issue personal or work email addresses to pupils or contact pupils.
- Any e-mails containing sensitive or personal, identifiable data should be removed to a separate folder to avoid accidental disclosure.
- Any attachments saved that may contain personal information should only be saved onto school equipment.

School Website

- The contact details on any school website should be the school address, email and telephone number. Staff and pupil details or personal information is not to be published.
- The headteacher has overall editorial responsibility and ensures that the content is accurate and appropriate.
- Photographs that include pupils are selected carefully so that they do not enable individual children to be clearly identified.
- Pupil's full names are not used anywhere on the website.
- Written permission from parents/carers must be obtained before photographs of pupils are published on the website. This is done on entering school but can be updated at any time. Any parent who wishes to withdraw this permission should contact the school office.

Social networking and personal publishing

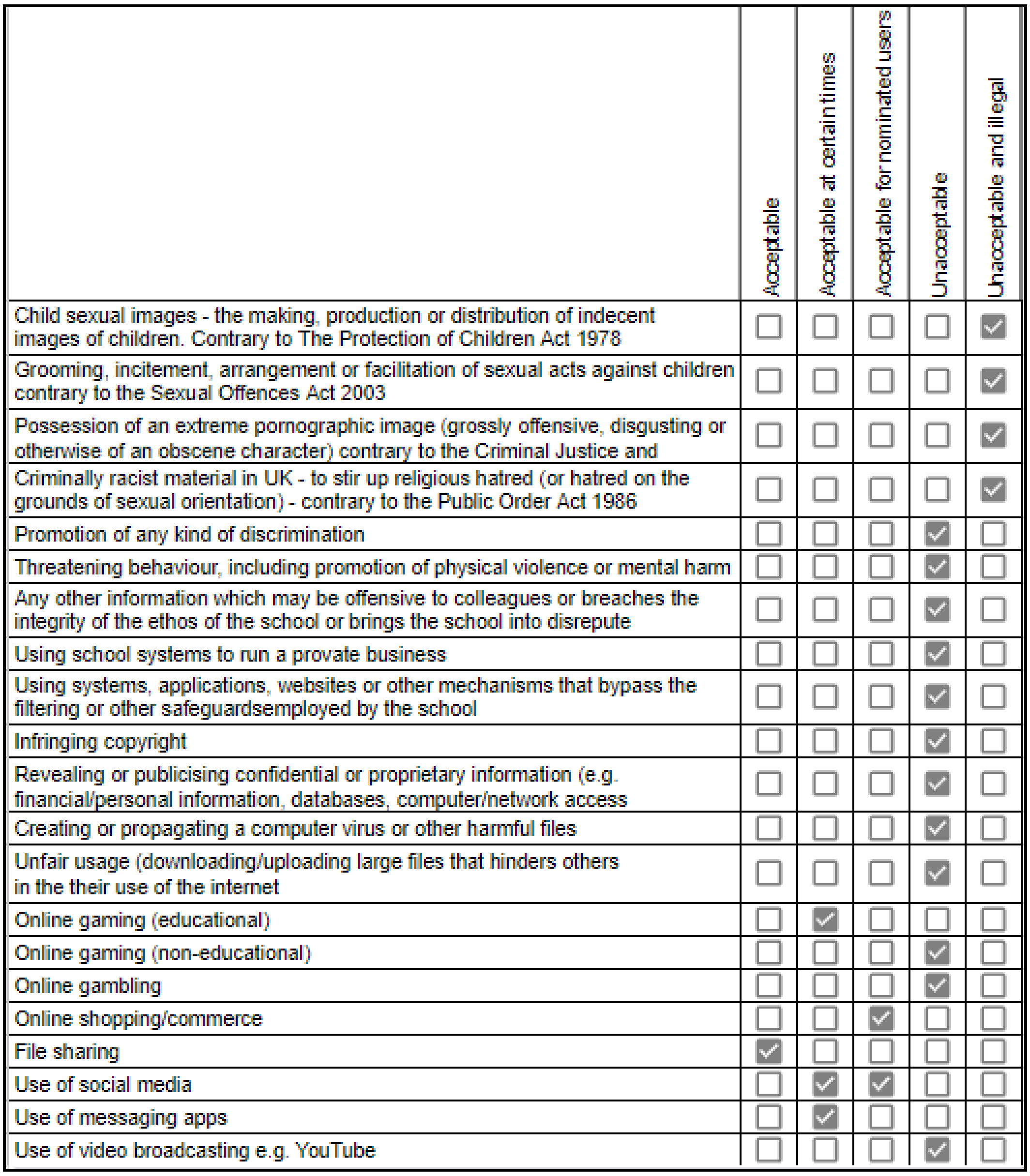
- Any social network sites used to support learning or links with other schools must be secure. They must be approved by the headteacher before use and any content uploaded should be checked by the teacher. The teacher is also responsible for pre-checking any content to be viewed by the children.
- The school blocks access to public social networking sites. Newsgroups are also blocked.
- Pupils are told never to give information which may allow them to be identified.
- Parents are invited to online safety events which advise that the use of social network sites (as well as other digital media) outside school brings a range of dangers for primary aged pupils.
- Parents are given the opportunity to suggest training or information requirements that they may have regarding Online safety.
- Staff are provided with guidance to support their safe use of social networking sites out of school through the Staff Social Network policy and County Council Guidelines.

Unsuitable/inappropriate activities

Some internet activity is illegal and would obviously be banned from school 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 a school context, either because of the age of the users or the nature of those activities.

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

User Actions 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:



	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual images - the making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978	□	□	□	□	☑
Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003	□	□	□	□	☑
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and	□	□	□	□	☑
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	□	□	□	□	☑
Promotion of any kind of discrimination	□	□	□	☑	□
Threatening behaviour, including promotion of physical violence or mental harm	□	□	□	☑	□
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	□	□	□	☑	□
Using school systems to run a provate business	□	□	□	☑	□
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguardsemployed by the school	□	□	□	☑	□
Infringing copyright	□	□	□	☑	□
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access	□	□	□	☑	□
Creating or propagating a computer virus or other harmful files	□	□	□	☑	□
Unfair usage (downloading/uploading large files that hinders others in the their use of the internet	□	□	□	☑	□
Online gaming (educational)	□	☑	□	□	□
Online gaming (non-educational)	□	□	□	☑	□
Online gambling	□	□	□	☑	□
Online shopping/commerce	□	□	☑	□	□
File sharing	☑	□	□	□	□
Use of social media	□	☑	☑	□	□
Use of messaging apps	□	☑	□	□	□
Use of video broadcasting e.g. YouTube	□	□	□	☑	□

Responding to incidents of misuse

- If staff or pupils discover an unsuitable site, it must be reported immediately to the teacher and then the Online Safety Co-ordinator, who will report the site to the appropriate person in the local authority (Richard Taylor/John Devlin) according to the safety incident flow chart displayed in the staff room. Following the flow chart, if it is felt that the incident is a child protection issue; this will immediately be reported to the headteacher and LCSB as necessary.
- If an incident involves extremist material, the Police should also be notified as well as the LSCB if it is felt that the access has been deliberately sought.
- All internet access including emails will be monitored through SENSO on the curriculum network. The admin system is protected by a separate firewall system.
- Regular updates from the local authority providing guidance for the safe use of technologies are acted on as it is received.

Mobile Phones and Mobile Devices

- In order to ensure the safety of both children and staff, mobile phones and other mobile devices should not be visible in the vicinity of children during the school day. Mobile phones should not be used during teaching sessions. If it is felt necessary to make phone calls/take messages during the school day this must occur during lunch / break times in an areas where there are no children (eg empty classroom/staff room). This is to safeguard teachers as well as pupils.
- Staff should not give out personal mobile numbers to pupils.
- Pupils are not permitted to bring mobile phones and other devices with photographic/video capability (eg ipods) into school except with the express permission of the Headteacher/senior staff.
- Pupils in Year 4 and above who begin walking home unaccompanied will be allowed to bring phones into school for their safety if parents read and sign the mobile phone policy. This will be on the understanding that the phones will not be turned on while in the school building, are kept by the teacher in a locked, safe place and are brought in at the owners' risk. Infringement of these rules will result in the phone being confiscated for the duration of the school day and parents contacted.
- As part of the children's online safety education, children are taught how to respond in the instance of receiving malicious messages or texts.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying 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 implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, 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.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Parents on school visits will be instructed not to take photographs on personal devices

Data Protection

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition. Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 and is:

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

Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used. The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our "Privacy Notice" and lawfully processed in accordance with Horton Grange's conditions for processing procedures.
- Personal and sensitive data relating to pupils or staff is not emailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the GDPR.
- Data subjects have a right to access their data and there are clear procedures for this.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- Only cloud storage that meets the requirements laid down by the Information Commissioner's office is used to store personal data.
- The staff acceptable use policy clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.

Staff ensure that they

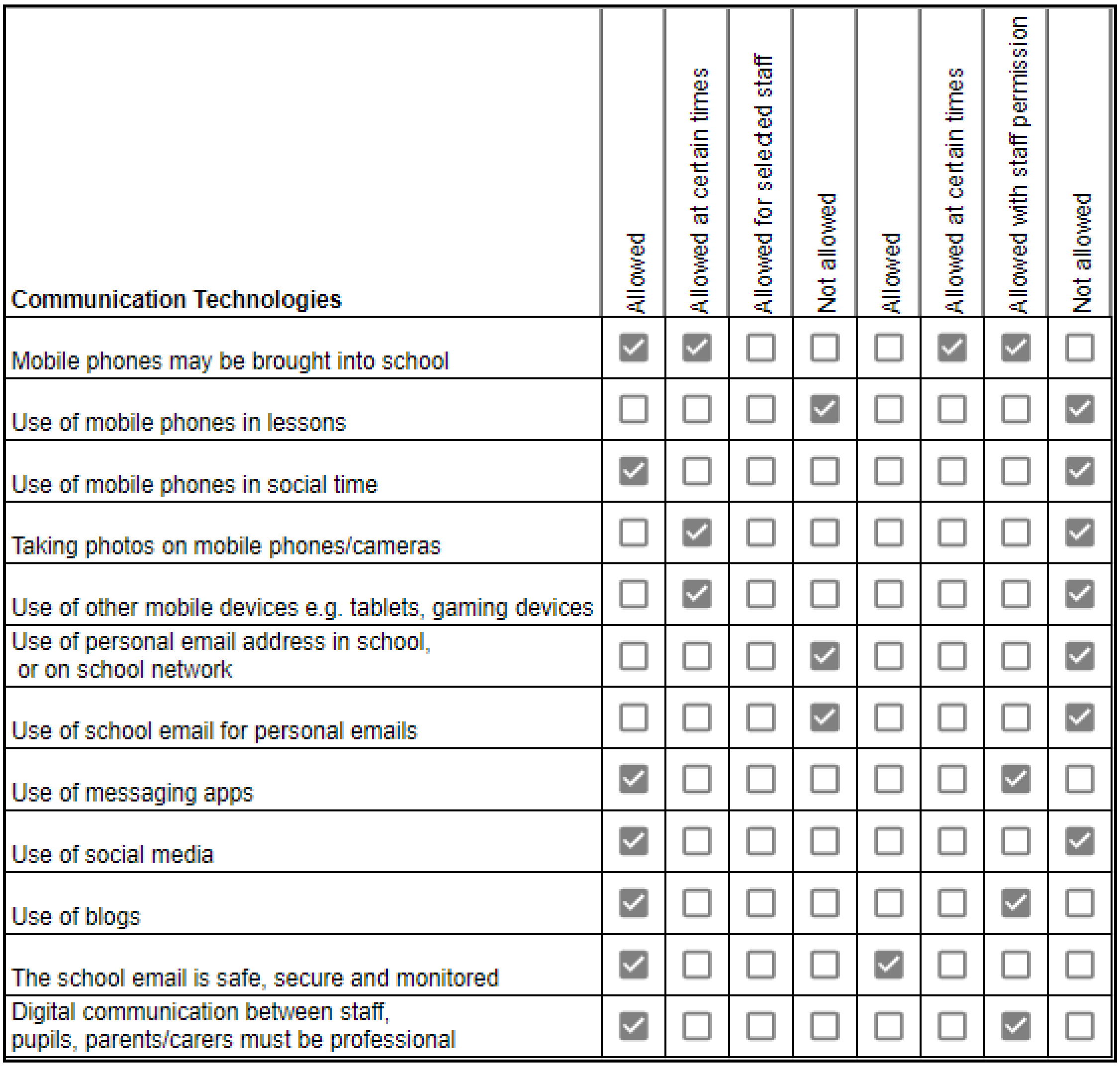
- Take care to ensure the safekeeping of personal data and minimise the risk or loss or misuse
- Use personal data only on secure password protected computers and devices and log off at the end of every session
- Transfer data using encryption and secure password protected devices

Where personal data is stored on removable media:

- The data is encrypted and password protected
- The device is password protected
- The device has approved virus and malware checking software
- The data is securely deleted from the device once finished with.

4. Managing Technologies

Emerging technologies are evolving at a rapid rate and although every attempt is made to protect children from offensive or inappropriate material and misuse, there may be occasions when inadvertent access occurs. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:



Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought into school	☑	☑	□	□	□	☑	☑	□
Use of mobile phones in lessons	□	□	□	☑	□	□	□	☑
Use of mobile phones in social time	☑	□	□	□	□	□	□	☑
Taking photos on mobile phones/cameras	□	☑	□	□	□	□	□	☑
Use of other mobile devices e.g. tablets, gaming devices	□	☑	□	□	□	□	□	☑
Use of personal email address in school, or on school network	□	□	□	☑	□	□	□	☑
Use of school email for personal emails	□	□	□	☑	□	□	□	☑
Use of messaging apps	☑	□	□	□	□	□	☑	□
Use of social media	☑	□	□	□	□	□	□	☑
Use of blogs	☑	□	□	□	□	□	☑	□
The school email is safe, secure and monitored	☑	□	□	□	☑	□	□	□
Digital communication between staff, pupils, parents/carers must be professional	☑	□	□	□	□	□	☑	□

5. Policy Decisions

- All staff and pupils must agree to the acceptable use policy in ICT agreement which forms part of the staff induction process and on the desktop screen following the login procedure.
- The AUP is regularly explained to the children at their level to ensure their understanding.
- The AUP is included in the home/school agreement to ensure that parents are aware of the high priority that the school places on safe use of technologies. It is also displayed in areas where computers are present.
- SENSO reports are regularly monitored by the Online Safety Co-ordinator who in turn reports to the senior management.
- The school keeps a record of all staff and pupils who are granted internet access.
- At key stage 1 /Early Years, access to the internet will be by adult demonstration with directly supervised access to approved online materials.
- At KS2, access to the internet will be by supervised access to online materials filtered by SENSO.

6. Assessing Risks

- The school takes all reasonable precautions to ensure that users access only appropriate material through the use of Lightspeed systems. Supervised access is recommended as the school is aware that no firewall system is completely infallible.
- The school audits ICT provision on an annual basis, or when new technologies are introduced to establish if the online safety policy is adequate and that its implementation is effective

7. Handling Online Safety Complaints

- The Online Safety Co-ordinator will inform class teachers if it is felt that there has been an infringement of the AUP by a child in the class. Minor infringements will first result in a warning given to the child. Further or more serious infringements will be dealt with under the school's behaviour policy.
- Any infringement of the school policy by pupils or staff which is deemed to be a child protection issue will immediately be reported to the appropriate authorities. Where this involved a member of staff, disciplinary procedures will be instigated.
- Incidents where staff or pupils are suspected of having obscene images on a mobile device will be dealt with via the NCC flow chart system and via the disciplinary procedures.