HINTON ST GEORGE
CHURCH of ENGLAND FIRST SCHOOL

'Let Your Light Shine'

ONLINE SAFETY POLICY

Review Date: January 2020
Frequency of Review: Every two years
Next Review Date: January 2022

Signed _____
on behalf of the Governing Body

Model School Online Safety Policy
September 2018 amended September 2019

Hinton St George CE First School

This Policy should be taken and used as part of Hinton St George Church of England School's overall strategy and implemented within the context of our vision, Instrument of Government aims and values as a Church of England School.

This Policy statement has been formally adopted by the governing body, in consultation with the Headteacher, and will be reviewed at the frequency recorded on this cover page.

Contents

Scope of policy
This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

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 such as cyber-bullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but are linked to membership of the school.

Keeping Children Safe 2019 [0]sets out specific responsibilities for governing bodies to ensure:

- children are taught about online safety (para 88)
- appropriate filters and appropriate monitoring systems are in place (para 87)
- online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach (page 98)

The school will manage Online Safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate Online Safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review
The implementation of the Online Safety Policy will be monitored by the teaching staff and Headteacher, meeting termly and reporting to the Governors annually.

The impact of the policy will be monitored by looking at:

- the log of reported incidents
- the internet monitoring log
- surveys or questionnaires of learners, staff, parents and carers
- other documents and resources
- future developments

0
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/830121/Keeping_children_safe_in_education_060919.pdf

Roles and responsibilities

The Headteacher and Governors oversee the safe use of technology when children and learners are in their care and act immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online and the prevention of being drawn into terrorism) of all members of the school community. They have concern for the online reputation of the school.

The class teachers will work with the Headteacher/Designated Safeguarding Lead (DSL) to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

The teachers and Headteacher will monitor the Online Safety Policy and AUPs (Acceptable User Policies) with a governor, member of the support staff and the school council. Pupils are an important part of this group, working with them through the school council, to contribute their knowledge and use of technology. They meet on a termly basis.

Role	Responsibility
Governors	• Monitor the effectiveness of the Online Safety Policy • Delegate a governor to act as Online Safety link • Online Safety Governor works with the Headteacher and teachers to carry out regular monitoring and report to Governors • Verify that the filtering, monitoring and or supervision systems are in place to identify children accessing or trying to access harmful and inappropriate content online
Headteacher/ Class Teachers	• Ensure that all staff receive suitable CPD to carry out their Online Safety roles including online risks of extremism and radicalisation • Create a culture where staff and learners feel able to report incidents • Ensure that there is a progressive Online Safety curriculum in place - monitor • Ensure that there is a system in place for monitoring Online Safety • Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious Online Safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented and review accordingly • Use an audit[0] to annually review Online Safety with the school's technical support • Meet with Online Safety Governor to discuss incidents and developments • Attend updates, subscribe to appropriate newsletters and liaise with the LA Online Safety staff and technical staff
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand, sign and act in accordance with the AUP and Online Safety Policy • Report any suspected misuse or concerns to the Designated Safeguarding Lead (DSL) or Deputy Designated Safeguarding Lead (DDSL) and check this has been recorded • Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum

0 https://staffonly.somerset.org.uk/sites/edtech/Subscriber%20Only/Questions%20for%20Technical%20Support%20v4.pdf

	• Model the safe, positive and purposeful use of technology • Monitor the use of technology in lessons, extracurricular and extended school activities • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident
Pupils	• Read, understand, sign and act in accordance with the Pupil AUP / agreed class internet rules • Report concerns for themselves or others • Make informed and positive choices when using technology in school and outside school, considering the effect on themselves and others
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss Online Safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the internet • Keep up to date with issues through newsletters and other opportunities • Inform teacher / Headteacher of any Online Safety concerns • Use formal channels to raise matters of concern about their child(ren)'s education • Maintain responsible standards when referring to the school on social media
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack • Ensure users may only access the school network using an approved password • Maintain and inform the Headteacher of issues relating to filtering • Keep up to date with Online Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety Leader for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities
Community Users	• Sign and follow the Guest/Staff AUP before being provided with access to school systems • Demonstrate appropriate standards of personal and professional conduct in line with the AUP • Use the Online Compass tool to review Online Safety

Education of pupils

'Children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum.'

Keeping Children Safe 2019

A progressive planned Online Safety education programme takes place in line with 'Teaching online safety in schools[0]', through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured through reference to UKCCIS Education for a Connected World framework[0] and is implemented through the use of Somerset ActiveBYTES scheme[0].

Within this:

- key Online Safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all teaching
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset ActiveBYTES scheme of work
- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- in lessons where internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches
- pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- the online safety coordinator maintains and passes on knowledge of current concerns to be included within learning experiences
- pupils are provided with opportunities to influence the online safety curriculum
- pupils will write and sign an AUP for their class at the beginning of each school year, which will be shared with parents and carers
- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying' and given opportunities to support each other
- a continuous provision map is used with the youngest learners and SEND learners to establish appropriate habits for responsible use of technology

[0] https://www.gov.uk/government/publications/teaching-online-safety-in-schools

[0] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/680356/Education_for_a_Connected_World2.pdf

[0] https://www.somerset.org.uk/sites/edtech/SitePages/e-Safety/ActiveBYTES.aspx

Education and information for parents and carers
Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear AUP guidance which they are asked to sign with their children
- providing regular newsletter items and appropriate support materials
- raising awareness through activities planned by pupils
- inviting parents to attend activities such as Online Safety week, Online Safety assemblies or other meetings as appropriate
- providing and maintaining links to up to date information on the school website

Education of wider school community
The school provides information about Online Safety to organisations using school facilities, local play groups and nurseries and members of the wider community which where appropriate include:

- details about the Online Compass review tool
- Online Safety messages targeted to grandparents and other relatives

Training of Staff and Governors
There is a planned programme of Online Safety training as part of the overarching safeguarding approach, in line with Keeping Children Safe 2019 (paragraph 84 and page 98) for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- all staff knowing the Designated Safeguarding Lead and Deputy Designated Safeguarding Lead and their responsibilities
- an annual audit of the Online Safety training needs of **all** staff
- **all** new staff and governors receiving Online Safety training as part of their induction programme
- providing information to supply and student teachers on the school's Online Safety procedures
- receiving regular updates through attendance at training sessions and by reviewing regular Online Safety newsletters from the LA
- this Online Safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings
- providing training within safeguarding training and as specific online safety updates and reviews
- providing guidance as required to individuals and seeking LA support on issues
- staff and governors are made aware of the Professionals Online Safety Helpline (POSH) 0344 381 4772

Online bullying

Online bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

The school will follow procedures in place to support anyone in the school community affected by online bullying.

Pupils and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by; telling a trusted adult, Online bully box, Childline App and phone number 0800 1111, POSH helpline 0344 381 4772.

Pupils, staff and parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.

All incidents of online bullying reported to the school will be recorded by the school.

The school will follow procedures to investigate incidents or allegations of online bullying.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with the school to support the approach to online bullying and the school's Online Safety ethos.

Sanctions for those involved in online bullying will follow those for other bullying incidents as indicated in the schools Behaviour Policy or AUP and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content
- internet access being suspended at the school for a period of time.
- the parent and carers of pupils being informed
- the police being contacted if a criminal offence is suspected

Sexting

The school will follow UKCCIS[0] advice on how to respond to an incident. We will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead (DSL). An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) will record any incident of sexting and the actions taken in line with advice from Somerset Local Authority.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

0 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647389/Overview_of_Sexting_Guidance.pdf

Technical Infrastructure
The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- the School ICT systems are managed in ways that ensure that the school meets Online Safety technical requirements

- there are regular reviews and audits of the safety and security of school ICT systems.

- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

    - ensuring ongoing backups take place and, in case of an incident, the school can restore data in line with our business continuity plan

    - the downloading of executable files by users

    - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school

    - the installing of programs on school devices unless permission is given by the technical support provider or Computing/ICT coordinator

    - the use of removable media (e.g. memory sticks) by users on school devices. (see School Personal Data Policy for further detail)

    - the installation of up to date anti-virus software

- access to the school network and internet will be controlled with regard to:

    - users having clearly defined access rights to school ICT systems through group policies

    - users being provided with an appropriate username and password (considering accessibility of users with particular needs where supervision is put in place to monitor activity)

    - staff users being made aware that they are responsible for the security of their username and password which they are required to change every 60 days; they must not allow other users to access the systems using their log on details

    - the 'master/administrator' passwords are available to the Headteacher and kept in the school safe

    - users must immediately report any suspicion or evidence that there has been a breach of security

- an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. Anyone allowed unsupervised access must sign the staff AUP and be made aware of this Online Safety Policy

- the internet feed will be controlled with regard to:
  - the school's responsibility[0] to "ensure appropriate filters and appropriate monitoring systems are in place. Children are safeguarded from potentially harmful and inappropriate online material." Keeping Children Safe 2019
  - Foundation Stage and Key Stage 1 pupils' access will be supervised with access to specific and approved online materials
  - Key Stage 2 pupils' will be supervised. Pupils will use age-appropriate search engines and online tools and activities
  - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged[0]
  - user based filtering used to provide differentiated access for staff and pupils
  - filtering issues being reported immediately
- the IT System of the school will be monitored with regard to:
  - the school IT technical support regularly monitoring and recording the activity of users on the school IT systems
  - Online Safety incidents being documented and reported immediately to the Designated Safeguarding Lead (DSL) who will arrange for these to be dealt with immediately in accordance with school policies

[0] https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring
[0] https://www.somerset.org.uk/sites/edtech/eSafety/Filter/Benefit%20Analysis%20request%20for%20unfiltering%20a%20website.pdf

Data Protection

The school's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

The school will:

- at all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates
- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- provide staff with secure equipment/services to store or transfer data eg remote access, One Drive, SharePoint school portal, encryption and secure password protected devices
- remove data in line with the school's Data Retention Policy
- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead and that relevant staff understand the full requirements of Data Protection Act 2018
- complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely

Use of digital images and sound

Photographs, video and sound recorded within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- build a culture where permission is always sought before a photo is taken or video and sound are recorded; including encouraging pupils to seek permission from other pupils to take, use, share, publish or distribute images and sound
- ensure verifiable permission[0] from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on the school website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use
- when using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images, record video and sound to support educational aims, following the school policy regarding the sharing, distribution and publication of

0 https://staffonly.somerset.org.uk/sites/edtech/Data%20Protection/Data%20Protection%202018/Documentation/eLIM%20IRMS%20Pupil%20Image%20Consent%20Form%202019.docx

those. School equipment only is used. Personal equipment of staff is not allowed for this purpose

- make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care 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

- make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed

- ensure that pupils' full names will not be used anywhere on the school website, school blogs or within school branded social media, particularly in association with photographs

- not publish pupils' work without their permission and the permission of their parents or carers

- only hold digital/video images on school approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the schools Data Retention Policy

- in accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at school events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images or in the sound recording. We ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before an event as to the expectations of the school

- make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the settings Online Safety Policy and will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people

Communication (including use of Mobile Devices and Social Media)
A wide range of communications technologies increases effective administration and has the potential to enhance learning. The school will:

with respect to email

- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that governors use a secure email system
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- make users aware that email communications will be monitored by the school
- inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- teach pupils about email and other communication tools alongside online safety issues through the scheme of work and implementation of the AUP
- only publish official staff email addresses where this required
- protect the identities of multiple recipients by using bcc in emails

with respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing

- enable online learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school
- control access to social media and social networking sites in school
- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences
- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given
- make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Headteacher/Senior Teacher
- ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content
- discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of

safe and professional behaviour in line with DfE advice[0], being careful about subjects discussed online

- staff are advised that no reference should be made to pupils, parents/carers or school staff on their personal social networking accounts

- register concerns (e.g. recording in Online Safety log) regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites

- support staff to deal with the consequences of hurtful or defamatory posts about them online

- inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the Headteacher

with respect to personal devices ***(including consideration of Keeping Children Safe 2019[0])***

- inform staff that personal devices should only be used at break and lunchtimes in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher (turned off at other times)

- ensure that staff understand that the AUP will apply to the use of their own portable / wearable device for school purposes

- inform staff and visitors that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Headteacher

- check any use of a personal device for an education purpose (where permission has been given) only uses the school's internet connection on the school site

- remind all that personal devices should be pin code or fingerprint protected and not discoverable by third parties

- advise staff not to use their personal mobile phone to contact pupils, parents and carers

- provide a mobile phone for activities that require them

- challenge staff and visitors when there is suspected misuse of mobile phones or devices

[0] DfE Cyberbullying Advice for headteachers https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf and Teaching Standards 2012 https://www.gov.uk/government/publications/teachers-standards

[0] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/830121/Keeping_children_safe_in_education_060919.pdf page 97

The following table shows how the school considers the way these methods of communication should be used.

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selecte staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones/wearable technology in school		x						x
Use of mobile phones/wearable technology in lessons		x						x
Use of mobile phones/wearable technology in social time	x							x
Taking photos on mobile phones or other camera devices		x				x		
Use of personal devices including wearable technology		x						x
Use of 'always on' voice activated technology		x						x
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of chat facilities, forums and closed groups in apps		x						x
Use of messaging apps		x						x
Use of social networking sites including live broadcasting				x				x
Use of blogs		x						x
Use of Twitter		x						x
Use of video broadcasting e.g. YouTube				x				x

Assessment of risk
Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the Online Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material

The school provides appropriate filtering and monitoring as stated in this policy. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school device.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to incidents
The school will follow Somerset's incident flowchart to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of child abuse, the investigation will be referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content)

- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded

- The Designated Safeguarding Lead (DSL) will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures

- The school will manage Online Safety incidents in accordance with the School Behaviour Policy where appropriate

- The school will inform parents and carers of any incidents or concerns in accordance with school procedures

- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required

- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Somerset Children Safeguarding Team and escalate the concern to the police

- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Education Safeguarding Advisor or Local Authority Designated Officer (LADO).

If an incident or concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Advisor to communicate to other schools in Somerset.	Education Safeguarding Adviser Jane Weatherill *Via Somerset Direct where pupil involved*
Should serious Online Safety incidents take place, the following external persons and agencies should be informed:	Local Authority Designated Officer (LADO) Anthony Goble *Via Somerset Direct where staff involved* Police

The police will be informed where users 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

- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation

- adult material that potentially breaches the Obscene Publications Act in the UK

- criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

Sanctions and Disciplinary proceedings
Sanctions and disciplinary procedures may be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation (p 17):

- child sexual abuse images
- grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity including radicalisation and terrorism
- 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 private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

In addition, the following indicates school policy on these uses of the internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Online gaming (educational)		x		
Online gaming (non-educational)			x	
Online gambling				x
Online shopping / commerce			x	
File sharing (using p2p networks)				x

Sanctions: Pupils

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. These are applied through the school's Behaviour Policy.

Schools should populate the grid below marking appropriate possible sanctions.
Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, ticks may appear in more than one column.
The ticks in place are actions which must be followed.

Incidents	Refer to class teacher / tutor	Refer to Head of Department / Hea of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network /internet acces 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).				✓		✓			
Unauthorised use of non-educational sites during lessons	✓							✓	
Unauthorised use of mobile phone / wearable technology / personal tablet	✓					✓		✓	
Unauthorised use of social networking / instant messaging / personal email	✓					✓		✓	
Unauthorised downloading or uploading of files	✓					✓		✓	
Allowing others to access school network by sharing username and passwords	✓					✓		✓	
Attempting to access or accessing the school network, using another pupil's account	✓					✓		✓	
Attempting to access or accessing the school network, using the account of a member of staff			✓			✓		✓	
Corrupting or destroying the data of other users			✓		✓	✓		✓	
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature			✓			✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions			✓			✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓			✓	✓		✓
Using proxy sites or other means to subvert the school's filtering system			✓		✓	✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident			✓		✓	✓	✓		✓
Deliberately accessing or trying to access offensive, pornographic or extremist material				✓		✓			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓			✓	✓		✓

Sanctions: Staff

Schools should populate the grid below marking appropriate possible sanctions.
Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, marks may appear in more than one column.
The marks in place are actions which must be followed.

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P)	Refer to Technical Support Staff fc action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).				L,P				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓				✓		
Unauthorised downloading or uploading of files		✓				✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓			✓	✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓				✓		
Deliberate actions to breach data protection or network security rules		✓						✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓						✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff		✓	✓					✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners				L				
Breech of the school Online Safety policies in relation to communication with learners				L				
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils				L				
Actions which could compromise the staff member's professional standing		✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓				✓		
Using proxy sites or other means to subvert the school's filtering system		✓			✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident				L				
Deliberately accessing or trying to access offensive or pornographic material, or material that seeks to radicalise				L				
Breaching copyright or licensing regulations		✓			✓	✓		
Continued infringements of the above, following previous warnings or sanctions		✓			✓			✓

Online Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- Computers and the network are only to be used for the purposes expressly permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and, where applicable, password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

HINTON ST GEORGE CHURCH of ENGLAND FIRST SCHOOL

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of each classes Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the pupils in their care.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent/Carer Permission Form

Parent / Carers Name: .....

Student / Pupil Name: .....

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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 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 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 online safety.

Signed: .....

Date: .....

Appendix C: Staff and Volunteer Acceptable Use Policy

HINTON ST GEORGE CHURCH of ENGLAND FIRST SCHOOL
Staff (and Volunteer)
Acceptable Use Policy Agreement School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies 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 access to the internet and digital technologies 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 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students / 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 systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology 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 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 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, unless I have permission to do so. Where these images are published (e.g. 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 social networking sites in school in accordance with the school's policies.
- 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.

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 (laptops / tablets / mobile phones / USB devices, etc.) 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 not have any personal mobile phones in the classrooms.
- I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- 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 ensure that my data is regularly backed up, in accordance with relevant school policies.
- 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, 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 / LA Personal Data Policy (or other relevant policy). 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 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.

When using the internet in my professional capacity or for school sanctioned personal use:

- 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 digital technology equipment in school, but also applies to my use of school 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.

I have read and understand the above and agree to use the school digital technology 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: