Stannington First School

E-Safety and Acceptable Use Policy (Staff and Pupils)

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.	Next review: March 2019
Should serious online safety incidents take place, the following external persons / agencies should be informed:	John Devlin (LA) LADO Anne Lambert (LA Safeguarding) Carol Leckie
Chair of Governors	Tim Hague

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Online Safety Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Community users

This policy has been developed in conjunction with guidance provided by SWGfL who consulted with groups including: the SWGfL E-Safety Group, Avon and Somerset Police, Plymouth University Online Safety

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires from the school community

Scope of the Policy

This policy applies to all members of the Stannington First School (including staff, students/ pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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 Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's published policies for Behaviour/Acceptable Use or E-safety.

Stannington First School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor, this role may is combined with that of the Child Protection / Safeguarding Governor.

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to FGB meeting

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 online safety will be delegated to the Online Safety Leader.
- The headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see NCC flow chart on dealing with online safety incidents).
- The headteacher is responsible for ensuring that the Online Safety Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. T
- The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The headteacher will receive regular monitoring reports from Online Safety Leader and NCC

Headteacher and Online Safety Leader

- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents
- ensure 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
- liaises with school technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- **attends relevant meetings**

Technical staff:

The Technical Staff member is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety 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 network filtering is applied and updated on a regular basis
- 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 / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher Online Safety Leader for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in LA 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, Online Safety Leader/ Officer for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / 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

Designated Safeguarding Lead / Designated Person / Officer

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

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

Students / Pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's 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 parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records

Community Users

Community Users who access school systems / website / Learning Platform as part of the wider school provision will be expected to sign a Visitor Acceptable Use Agreement before being provided with access to school systems.

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.

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 /PHSE or other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, 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 or NCC 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

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, Learning Platform*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications* *http://www.childnet.com/parents-and-carers*

Education – The Wider Community

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

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide online safety information for the wider community*
- *Supporting community groups e.g. Tree Tots Toddlers*

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 online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.

- The Online Safety Leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Leader will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

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

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

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.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements outlined in Local guidance

- 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 systems and devices.
- All users will be provided with a username and secure password by the class teacher who will keep an up to date record of users and their usernames.
- Users are responsible for the security of their username and password. EYFS and Year 1 will have a picture/colour password
- The “master / administrator” passwords for the school / academy ICT system, used by the Network Manager must also be available to the Headteacher and Online Safety leader leader and kept in a secure
- The 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

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- 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, see 'Reporting an E-Safety incident' 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.
- Temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems is granted after agreement of the Acceptable Use Policy and monitored in the usual way
- This policy guidance applies to school devices used out of school. Staff must ensure the protection of information accessed outside of school and this information must not be transferred to personal devices.
- Only the school technician may download executable files and install programmes on school devices.
- Removable media (eg memory sticks / CDs / DVDs) must not be used unless safely encrypted. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / 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.

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. However, the use of BYOD should not introduce vulnerabilities into existing secure environments. There are a number of e-safety considerations for BYOD that require review before implementing this practice in our school. **At present no pupils are permitted to access their own devices on the school premises (including the use of Kindles for school reading)**

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers gives consideration to the use of mobile technologies and sets out clear expectations and responsibilities for all users
- All users are provided with and accept the Acceptable Use Agreement

- The school adheres to the Data Protection Act principles
- All network systems are secure
- Mandatory training is undertaken by all staff
- Pupils receive guidance on the use/misuse of personal devices
- Pupils are not allowed to wear smart watches
- Staff wearing a smart watch must ensure that their mobile phone is switched off and that their watch is not receiving text alerts/e-mails during the school day
- Staff mobile phones should be kept secure during the school day and switched off
- If staff use personal devices to access work e-mails, these will be subject to the monitoring required by NCC

School owned / provided devices:

- Laptops may be taken home by teaching staff to facilitate planning at home. These are subject to the same monitoring procedures that are used in school.

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 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
- 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 published / 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 academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy 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 / academy 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.

Data Protection

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

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

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- 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
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected – only use a device approved by NCC and provided by the school
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, once it has been transferred or its use is complete.
- Images will be transferred weekly to a secure school share (Cohort file) and these images will be deleted when a pupil leaves the school – unless this is of particular interest to the school and permission has been granted to keep the image

Communications

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

	Staff & other adults				Pupils			
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 to the school / academy	✓	✓						✓
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 addresses in school, or on school network				✓				✓
Use of school / academy email for personal emails				✓				✓
Use of messaging apps	✓						✓	
Use of social media	✓							✓
Use of blogs	✓						✓	
Smart watches	✓							✓
Fitbits	✓						✓	

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

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- **Users must immediately report, to the nominated person – in accordance with the, 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 students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) 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.

Social Media and Social Networking

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- Ensuring that appropriate use of the internet and social media forms part of the staff code of conduct

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information. Staff must ensure that they are using the highest possible privacy settings
- The school is not mentioned, by name, on personal social media accounts
- Are aware of the implications of being 'tagged' in other people's photographs
- No contact is made through social media with pupils or their siblings
- Postings on social media are not libelous or likely to bring the school and it's community into disrepute

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material 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.

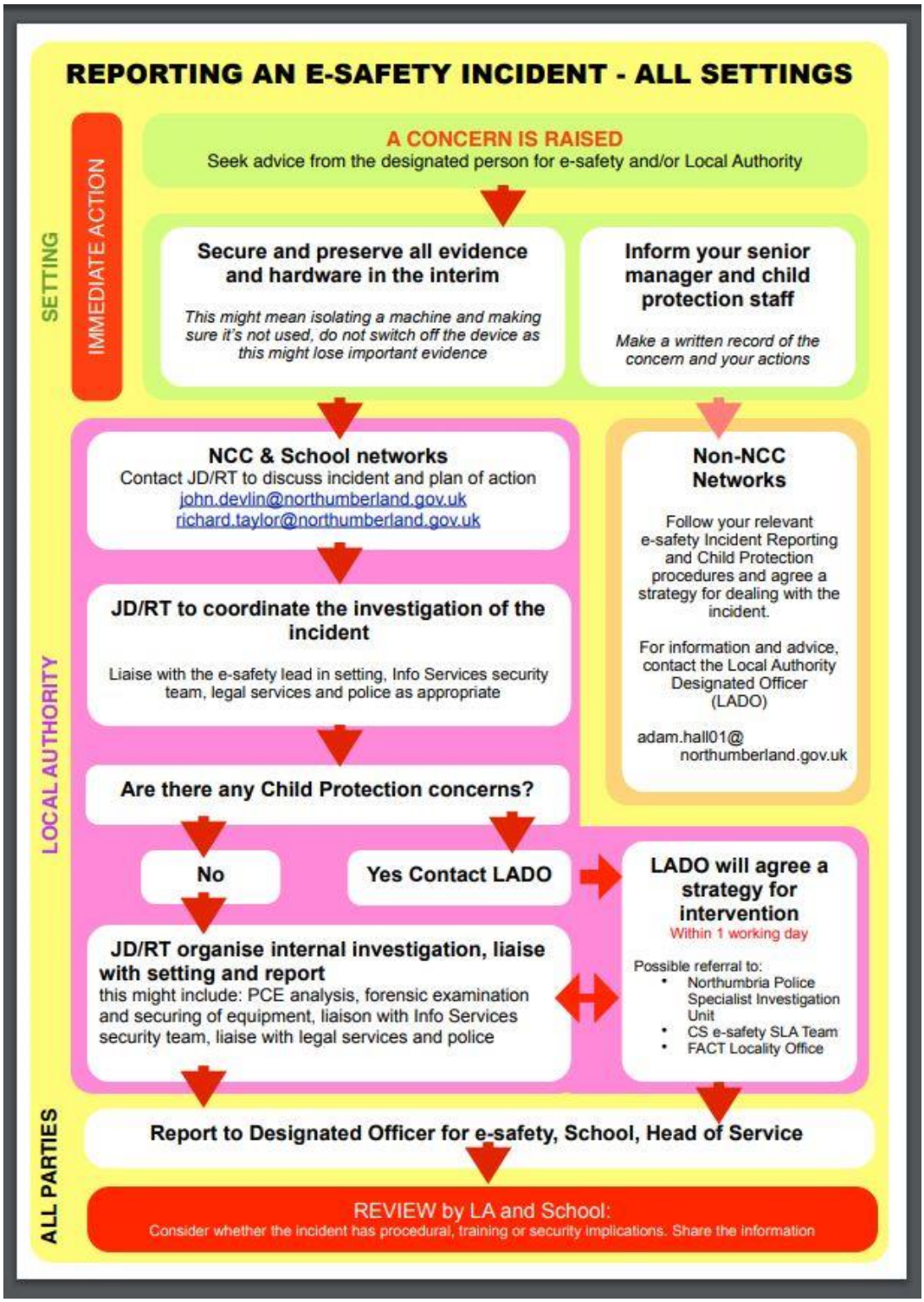
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

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	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing		X				
Use of social media			X	X		
Use of messaging apps			X			
Use of video broadcasting e.g. Youtube – selected by staff			X			

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement of Local Authority
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

Students / Pupils Incidents

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:	Refer to class teacher	Refer to Head teacher	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	X	X	X	X
Unauthorised use of non-educational sites during lessons		X		X	X	X		X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		X		X	X	X	X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X		X	X	X	X	X
Unauthorised downloading or uploading of files		X		X	X	X	X	X
Allowing others to access school network by sharing username and passwords		X		X	X	X	X	X
Attempting to access or accessing the school network, using another pupil's account		X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff		X		X	X	X	X	X
Corrupting or destroying the data of other users		X		X	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	X
Continued infringements of the above, following previous warnings or sanctions		X		X	X	X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school		X		X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	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	X	X

Staff Incidents

	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for 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).	X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X			X		
Unauthorised downloading or uploading of files	X	X		X	X		
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	X	X		X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X		
Deliberate actions to breach data protection or network security rules	X	X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	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	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X		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	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X	X	X

Acceptable Use Policy – Staff and Pupils

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Stannington First School**,** we understand the responsibility to educate our pupils on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for a school to use technology to benefit learners. Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet;

technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring
All internet activity is logged by the school's internet provider. These logs may be monitored by that provider.

Breaches
A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.
For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.
Policy breaches may also lead to criminal or civil proceedings.
The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

Incident Reporting
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access/PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

Computer Viruses
All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

ICT Acceptable Use Policy: Staff and Pupils

1. Introduction

The internet is a valuable resource that can raise educational standards by offering both pupils and teachers opportunities to search for information from a very wide range of sources based throughout the world. However, some of the information to be found on the internet will be inappropriate for pupils and we feel it is important to have a policy in place that takes this issue into account.
The school has a duty to ensure that before using the internet with pupils, staff have had the opportunity to discuss how they will deal sensitively with inappropriate use. The following policy helps to define appropriate and acceptable use by both staff and pupils and has been further discussed with Governors and pupils themselves.
Please also refer to our Safeguarding and Child Protection Policy and Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings.
The implementation of this policy is the responsibility of all members of staff.

2. The Internet in School

The internet is a powerful technology, and we realise that it must play an important role in any learning environment. Through the internet, teachers are able to find information on topics they may be teaching, worksheets that have been written by other teachers and newsgroups of a particular interest to the school, and they will be able to share ideas with teachers around the region, nationally and internationally too. It aids planning and collaboration between schools. It provides an e-mail address to members of staff to enable them to keep in ready contact with other schools.
Parents can contact staff members via the school admin email address:
admin@stannington.northumberland.sch.uk

3. The Internet in the Curriculum

The use of the Internet in the curriculum needs careful planning, and it should not be assumed that the children have the skills and knowledge of how to work safely in an online environment – for example, how to use search engines safely. Therefore, if the internet is to be used, the teacher should ensure that these points are covered in the interests of accessibility, and also of safety.

4. School Website

Stannington First School has a website and there are photographs which contain images of the children included in the content. Children in photographs are not identifiable by name (ie. there will not be any captions containing the children's names alongside photographs). If a child's name is mentioned elsewhere (for example, because of some work that is displayed on the website), only the first name will be used and it will not be linked to any photograph of the child or any other personal details.
The school does not publish personal email addresses of pupils or staff on the school website.

5. Roles and responsibilities

E-safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored. The Deputy Head is the e-safety lead and has completed online training.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

As the children progress through the school there is a gradual progression in access to the internet. Pupils will be made aware of unacceptable use of the internet without teachers being too explicit (as this may encourage some children to disobey the rules). The rules for using the internet will be made clear to all pupils and children will have to sign the Rules for Responsible Internet Use prior to using the internet. They will be made aware that if they feel that the rules do not apply to them and therefore decline to sign the agreement, then this will result in an instant loss of access to the internet.

The rules apply to staff as well as pupils and all staff (including temporary and regular supply teachers) will be asked to sign the Acceptable Use of the Internet form annually.

6. Monitoring

It is the role of both the Headteacher and Deputy Head to monitor and evaluate the overall effectiveness of internet use throughout the school and s/he will do this on a regular basis. Each teacher will be responsible for monitoring the use of the internet within their classroom and ensure that unacceptable material is not accessed. The Headteacher has responsibility for checking that no inappropriate material is on the school system and the children are made aware that teachers have access to all their folders of work. The coordinator also ensures that the computer system is regularly checked for computer viruses with the SOPHOS system, taking advice from the school's provider of technical support.

7. Managing the school network

The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network, or perform any other activities that the school may see fit.

8. Personal Use

The computers, electronic media and services provided by the school are primarily for educational use to assist staff in the performance of their job. Limited or incidental use of electronic media for personal purposes is acceptable, and all such use should be done in a manner that does not negatively affect the system's use for their educational purposes. However, staff are expected to demonstrate a sense of responsibility and not abuse this privilege. Staff are responsible for the physical security of school devices and these should not be used by other family members.

No personal devices should access the school's wireless internet without permission from the Headteacher.

Personal devices used to access school e-mail must be password protected and log out automatically. Staff must be aware of their surroundings when accessing personal information and e-mails to ensure that information cannot be read by other people. E-mails that contain sensitive or personal information should be moved to separate folders, once processed, to reduce the risk of unauthorised disclosure.

Attachments to e-mails, containing personal information, should be saved on to school equipment only.

Stannington First School expects any staff using social media sites to ensure that their use is conducive to their professional status. They should not mention the school by name or in passing, or discuss individuals or groups within the school, or compromise the school values.
In addition, staff must ensure that any private blogs, bulletin boards, websites etc. which they create, or actively contribute to, do not compromise, and are not confused with, their professional role.
Staff must ensure that any engagement in any online activities does not compromise their professional responsibilities.

- No reference should be made in social media to pupils, parents / carers or school staff
- Staff must not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles must be regularly checked to minimise risk of loss of personal information. Staff must ensure that they are using the highest possible privacy settings
- Staff should be aware of the implications of being 'tagged' in other people's photographs
- Staff will make no contact through social media with pupils or their siblings
- Staff must ensure postings on social media are not libelous or likely to bring the school and it's community into disrepute

Additional Information – see Social Networking Guidance

Northumberland County Council – October 2017

Stannington First School Rules for Responsible Internet Use by Pupils

The school has installed computers, purchased iPads and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

Primary Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT in school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT or computing passwords
- I will only open/delete my own files
- I will not copy other people's work and say that it is my own.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not bring a Kindle or e-book reader to school as I am not allowed to use this during the day
- I will not sign up to online services until I am old enough [over 13 years old for many services]
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted

The school cannot accept any responsibility for access to the internet outside of school even if children are researching a topic related to school.

Early Years Pupil Acceptable Use Agreement / e-Safety Rules

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has 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 know that if I break the rules I might not be allowed to use a computer / tablet

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that high levels of data-protection are adhered to at all times. This means locking computers whilst leaving the room.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of another staff member
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this
- I understand this forms part of the terms and conditions set out in my contract of employment

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Full Name ……..... (printed) Signature ……
Job title …… Date ……..

Staff Professional Responsibilities

A clear summary of professional responsibilities related to the use of ICT which has been endorsed by unions.

PROFESSIONAL RESPONSIBILITIES
When using any form of ICT, including the Internet, in school and outside school

For your own protection unions advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and / or staff for professional purposes, in accordance with school policy and with the knowledge of another member of staff.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.
- You have a duty to report any e-Safety incident which may impact on you, your professionalism or your organisation

Acknowledgements
SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids