DOVECOTES PRIMARY SCHOOL

POLICY STATEMENT FOR E-SAFETY

for staff, children and parents

(Digital Safeguarding including Social Media)

SOUTH WEST GRID FOR LEARNING

UK Safer Internet Centre

360 degree safe

ONLINE SAFETY WITH PLYMOUTH UNIVERSITY

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by Dovecotes Primary School made up of:

- *Headteacher / Senior Leaders*
- *E-Safety Officer / Coordinator*
- *Computing / Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors / Board*
- *Parents and Carers*
- *Community users*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body:*	
The implementation of this e-safety policy will be monitored by:	*G.Beddow (E-Safety and Safeguarding Coordinator / Officer);* *L.Gould (Computing Coordinator)* *B.Evans (Media/website Coordinator)* *Senior Leadership Team*
Monitoring will take place at regular intervals:	*At least once per year*
The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*At least once per year*
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	*September 2020*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *students / pupils*
  - parents / carers
  - *staff*

Scope of the Policy

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements. It applies to all members of the *school* community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of Dovecotes Primary School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-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 line with Searching, Screening and Confiscation 2018. In the case of both acts, action can only be taken over issues covered by the Behaviour Policy.

Dovecotes Primary 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 e-safety behaviour that take place out of school in line with the Dovecotes Code of Conduct, Acceptable Usage Policies, Employee Handbook and Behaviour Policy. Guidance on Keeping Children Safe Online in line with 'Keeping Children Safe in Education' 2019 has also been adhered to and referenced in this document as well as the guidance from Teaching Online Safety in School 2019.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the *school*:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *E-Safety Governor* (G.Beddow – also Safeguarding Governor, T.Wakefield). The role of the E-Safety *Governor* will include:

- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors / meeting*

Headteacher and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator*.
- **The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures).
- *The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*
- *The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.*

E-Safety Officer:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety/Computing *coordinator* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Technical staff:

Technical Staff / Computing co-ordinator are 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 e-safety technical requirements and any *Local Authority / other relevant body* E-Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher / Senior Leader; E-Safety Officer* for investigation / action / sanction
- *that monitoring software / systems are implemented and updated as agreed in school / academy policies*

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up-to-date awareness of e-safety matters / current e-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 / Senior Leader ; E-Safety 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 (including social networking)*
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with unsuitable material found in searches*

Child Protection / Safeguarding (Gill Beddow)

should be trained in e-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

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding e-safety and monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the *Governors.*

Members of the *E-safety Group* (or other relevant group) will assist the *E-Safety Officer* with:

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Students / pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy**
- have good understanding of research and the need to avoid plagiarism/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 e-safety practice when using digital technologies out of school and realise that the *school's* E-Safety Policy covers their actions out of school, if related to their membership of the school

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 and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good e-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 and on-line student / pupil records
- their children's personal devices in the school (when this is allowed) in line with the school's Mobile Phone policy but following, where necessary Searching, Screening and Confiscation 2018.

Policy Statements

Education – students / 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned e-safety curriculum should be provided as part of Computing / PHSE / Irresistible Learning and other lessons and should be regularly revisited in line with Education for a Connected World by the UK Council for Child Internet Safety, 2018**
- **Key e-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 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 use of digital technologies / the internet / 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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 with monitoring software reporting violation to the DSL and designated staff to monitor such actions.*
- *Pupils are to adhere to the Mobile Phone Policy in line with the AUP.*

Education – parents / carers

Many parents and carers have only a limited understanding of e-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*
- *Parents / Carers evenings / sessions (at least one per year)*
- *High profile events / campaigns eg Safer Internet Day / E-Safety Awareness Day / Week*
- *Reference to the relevant web sites / publications*

Education – The Wider Community

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

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

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. Use of SWGfl includes unlimited online webinar training. (**http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development)
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements and are aware of and follow the Digital Safeguarding Policy, Mobile Phone policy, Code of Conduct, keeping in line with the Employee Handbook.**
- *The E-Safety Officer / Computing Co-ordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The E-Safety Officer / Computing Co-ordinator will provide advice / guidance / training to individuals as required.*

Training – Governors / Directors

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

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

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users (KS2) will be provided with a username and secure password** by *the Computing Co-ordinator who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username / password** *and will be required to change passwords regularly*
- **The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place**
- **The Computing Co-ordinator s 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.
- *The school has provided enhanced / differentiated user-level filtering*
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed and outlined to them in E-Safety training).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An appropriate system is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *Agreed guidelines are in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school. Agreed guidelines are also in place that allow staff to / forbids staff from downloading executable files and installing programmes on school devices. This includes the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.*

Bring Your Own Device (BYOD)

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. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments.

- The school has a set of clear expectations and responsibilities for all users outlined in the Mobile Phone Policy
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported

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 digital images and in particular the sharing and storing of digital images, particularly on the internet. NB: Please see Appendix for specific guidance in Social Media Policy. 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. 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 and such publishing in school or on school devices is strictly prohibited.**
- 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 comment on those involving other *pupils* in the video/images.
- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Written permission from parents/carers to be obtained before photographs are published to website.*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals / school into disrepute.*
- *Pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images, including parental consent.*
- *Pupils' full names will not be used on websites / blogs, particularly in association with photographs.*
- *Pupils' work can only be published with the permission of the pupil and parents or carers.*

Upskirting

As outlined in the school's Safeguarding and Child Protection policy and in line with 'Keeping Children Safe in Education' 2019, this typically involved taking a picture under a person's clothes without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification to cause the victim humiliation, distress or alarm. This is a criminal offence.

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

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
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

Communication Technologies	Staff & other adults				Students / Pupils				
	Allowed	At certain times	At head's discretion	Not allowed	Allowed	At certain times	With staff permission	Certain circumstances	Not allowed
Mobile phones may be brought to school	■								■
Use of mobile phones in lessons			■						■
Use of mobile phones in social / non-directed time	■							■	
Taking photos on mobile phones / cameras			■					■	
Use of other mobile devices eg tablets, gaming devices		■				■			
Use of personal email addresses in school, or on school network			■						■
Use of school email for personal emails			■						■
Use of messaging apps/social media				■					■
Use of blogs		■				■			

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 pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive / discriminatory/threatening/bullying in nature and must not respond to such communication.**
- **Any digital communication between staff and pupils or parents / carers (e.g. on Showbie, learning platform, emails, website, 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.*
- *Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use.*
- *Pupils should be taught about e-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 - Protecting Professional Identity

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 / academy* 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 limiting access to personal information:

- Training to include: 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

School staff should ensure that:

- No reference should be made in social media to the school in any way, including 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.

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

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

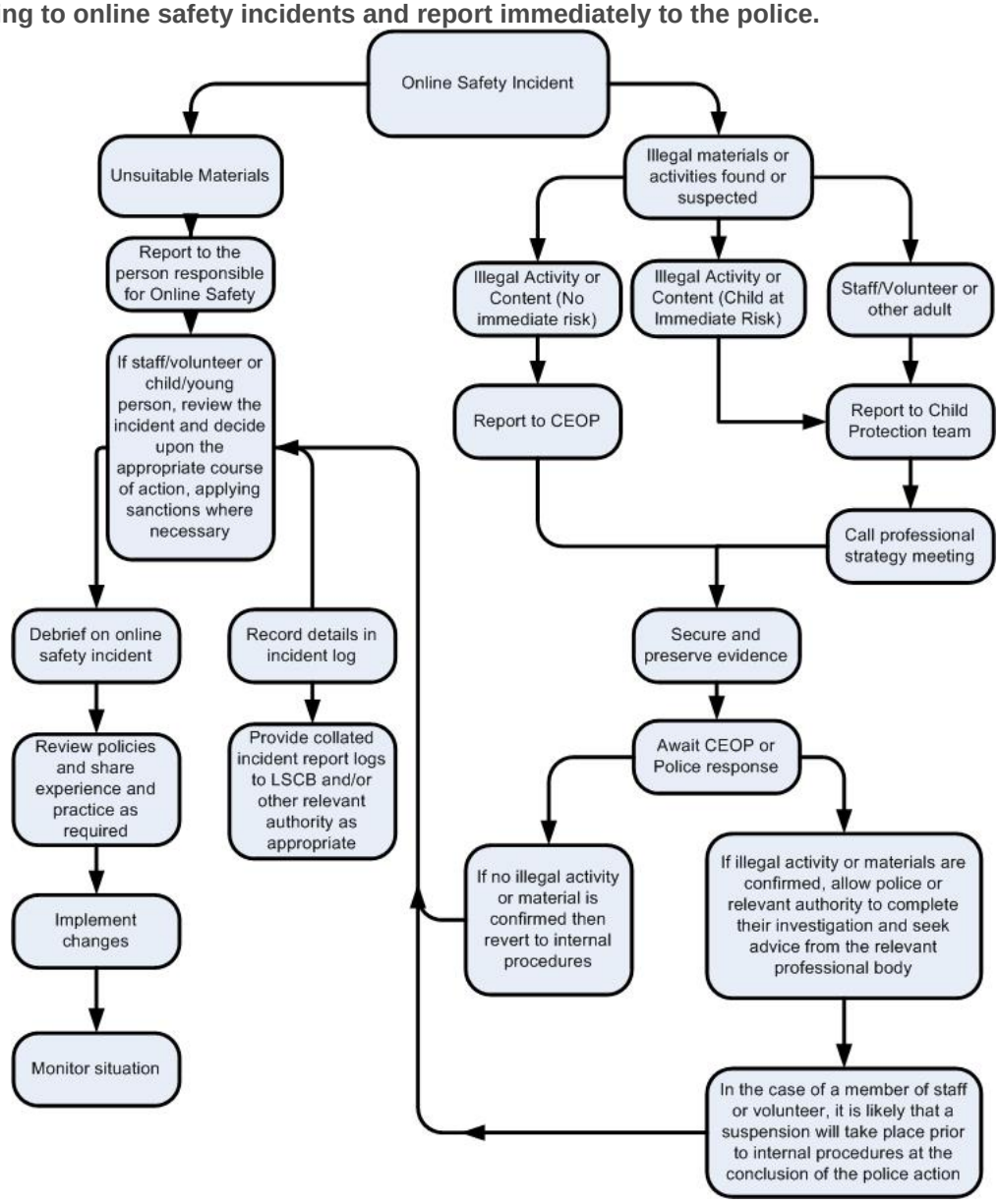
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child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

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

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 (below and appendix) 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 by Local Authority or national / local organisation (as relevant).
  - 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
  - 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 / academy* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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:

Students / Pupils

Incidents:	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. 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	
Unauthorised use of non-educational sites during lessons	X	X			X			
Unauthorised use of mobile phone / camera / mobile device	X	X			X			
Unauthorised use of social media / apps / 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	X	X		X	X		X	
Attempting to access or accessing the school network, using another student's / pupil's account	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	
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	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X	X	
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	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			

Staff Actions / Sanctions

Incidents:	Refer to Key Stage Coordinator	Refer to Deputy / 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
Inappropriate personal use of the internet / social media / personal email			x					X
Unauthorised downloading or uploading of files			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						
Careless use of personal data eg holding or transferring data in an insecure manner		X						
Deliberate actions to breach data protection or network security rules			x					X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x					X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x						
Actions which could compromise the staff member's professional standing		X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		x	x					X
Using proxy sites or other means to subvert the school's / academy's filtering system		X						
Accidentally accessing offensive or pornographic material and failing to report the incident		X						
Deliberately accessing or trying to access offensive or pornographic material			x	X				X
Breaching copyright or licensing regulations			X					X
Continued infringements of the above, following previous warnings or sanctions			x					x

Appendix

Copies of the more detailed template policies and agreements, used to form the basis of this policy, can be downloaded from:

http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

Copies of the AUPs for staff and children as well as Laptop Agreements for staff and AUP/agreements for parents can be found on the following pages.

Social Media Policy

Social media (including Facebook, Twitter, Instagram) is a general term for any online platform which enables people to interact, often in the public eye.

At Dovecotes Primary School, we recognise the benefits and opportunities that a social media presence can offer. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media however, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the staff parents, carers and children of Dovecotes Primary School.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements, which can be found at the end of this document.

This policy applies to all staff, parents/carers and children and any online communications which directly or indirectly represent or address the school. At Dovecotes Primary School, we respect privacy and understand that staff, parents and children may use social media for personal use. However, any communications that could have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Roles & Responsibilities

- **SLT will:**
  - Provide training and guidance on Social Media use;
  - Develop and implement the Social Media policy;
  - Take a lead role in investigating any reported incidents;
  - Make an initial assessment when an incident is reported and involve appropriate staff and external agencies if/as required;
  - Receive completed applications for Social Media accounts;
  - Approve account creation.
- **Administrator / Moderator will:**
  - Create the account following SLT approval;
  - Store account details, including passwords securely;
  - Be involved in monitoring and contributing to the account;
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring).
- **Staff will:**
  - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies;
  - Attend appropriate and regular training;
  - Regularly monitor, update and manage content posted via school accounts;
  - Add an appropriate disclaimer to personal accounts when naming the school.

Monitoring

Any school accounts created, including the website, must be monitored regularly and frequently, including during the holidays. Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day) even if only to acknowledge receipt. Regular monitoring is essential to eliminate or address inappropriate behaviour arises on social media.

Behaviour

- **Dovecotes Primary School requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies, including the Safeguarding policies, Code of Conduct, Employee Handbook and Behaviour policy.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about the school, its staff, parents/carers or children. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to the DSL and/or Computing/E-safety coordinator.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, offensive comments should be addressed and dealt with swiftly and with sensitivity;
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken;
- If you feel that you or someone else is subject to abuse by colleagues, parents/carers or children through use of a social networking site, then this action must be evidenced if appropriate and then reported using the agreed school protocols; the DSL (headteacher) can then address the matter accordingly.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages representing or on behalf of the school are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to:

- **Permission to use any photos or video recordings should be sought**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts or the website.**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.
- All images taken on behalf of the school, including those involving children, should be taken on a school approved device, **not** a personal device, in line with the Mobile Phone policy of the school.

Personal use

- **Staff**
  - **Staff are not permitted to follow or engage with current or prior children of the school on any personal social media network account.**
  - Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the staff thus school or 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 and in line with the Mobile Phone policy.
  - Personal communications which do not refer to (whether directly or indirectly) 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.
- **Children**
  - **Children are to be advised of the official guidelines and age restrictions on social media/networking sites and are therefore discouraged from having access to such accounts at a Primary School age.**
  - The school's education programme should enable the children to be safe and responsible users of social media.
  - Children are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy.
- **Parents/Carers**
  - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
  - **Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.**

Managing your personal use of Social Media:

- "Nothing" on social media is truly private;
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts;
- Check your settings regularly and test your privacy both on school and personal accounts;
- Keep an eye on your digital footprint;
- Keep your personal information private;
- Regularly review your connections – keep them to those you want to be connected to;
- When posting online consider; Scale, Audience and Permanency of what you post;
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school;
- Use a disclaimer when expressing personal views;
- Make it clear who is posting content;
- Use an appropriate and professional tone;
- Be respectful to all parties;
- Ensure you have permission to 'share' other people's materials and acknowledge the author;
- Express opinions but do so in a balanced and measured manner;
- Think before responding to comments and, when in doubt, get a second opinion (discuss with DSL);
- Seek advice and report any mistakes using the school's reporting process;
- Consider turning off tagging people in images where possible but always seek permissions.

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute;
- Don't publish confidential or commercially sensitive material;
- Don't breach copyright, data protection or other relevant legislation;
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content;
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content;
- Don't use social media to air internal grievances – follow specified procedures outlined.

Dovecotes Primary School - AUP for governors

This acceptable usage policy applies to governors' use and monitoring of technology systems and services provided or accessed as part of their role within Dovecotes Primary School both professionally and personally. This may include but is not limited to the use of laptops, mobile phones, tablets, digital cameras and email; networks and data storage and online and offline communication technologies. Governors must ensure technology use is consistent with the school ethos, code of conduct and Digital Safeguarding policies.

I, as a member of the governing board, will ensure that:

- the school has appointed an e-Safety coordinator and have a named e-Safety governor;
- a Digital Safeguarding Policy has been written by the school, taking into account the DFE statutory guidance 'Keeping Children Safe in Education' 2019, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' 2018 and the City of Wolverhampton's published processes and guidance.
- learners are encouraged to enjoy safe use of digital technology to enrich their learning;
- learners are made aware of risks and processes for safe digital use in line with the Digital Safeguarding Policy and, together with all necessary adults (including staff and parents), have received the appropriate acceptable use policies and any required training;
- parents will be informed that all technology usage of children may be subject to monitoring, including URL's, search engine history, social media and text in line with Searching, Screening and Confiscation 2018;
- the e-Safety policy and its implementation will be reviewed annually;
- the school internet access is designed for educational use and reasonable precautions will be taken to ensure only appropriate material is accessed by all users, including through appropriate filtering and monitoring;
- the school will monitor and review use of technology to establish if the e-Safety policy is adequate and appropriately implemented;
- methods to identify, assess and minimise risks will be reviewed annually;
- complaints of internet misuse will be dealt with by a senior member of staff, including conduct of staff, pupils', parents' and/or governors' use of social media.
- any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the Digital Safeguarding policy.
- security of documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, using the cloudw school learning platform to upload any work documents and files in a password protected environment.
- any school-related documents or files that have been lost, will be reported to the e-Safety governor/coordinator and Data Protection Officer as soon as possible.
- my online reputation and use of technological systems are compatible with my professional role, in line with the Dovecotes Code of Conduct, Digital Safeguarding and mobile phone policies. This includes use of email, text, social media or any other personal use. I will not engage in online activities or behaviour that could compromise professional responsibilities/bring the school's reputation into disrepute.

Signed ..... **Print** ..... **Date** .....

Dovecotes Primary School
AUP for school workforce

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users while supporting teaching and learning.

I agree that I will:

- only use personal data securely;
- implement the school's E-learning and Digital Safeguarding (inc. Social Media) policies;
- educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- educate pupils in the recognition of bias, unreliability and validity of sources;
- actively educate learners to respect copyright law;
- only use approved e-mail accounts in school;
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified;
- only use school devices to photograph or record pupils;
- only give access to appropriate users when working with blogs or wikis etc...;
- set strong passwords – a strong password is one which uses a combination of letters (both upper and lower case), numbers and other permitted symbols;
- report unsuitable content or activities to the E-Safety Coordinator;
- ensure that videoconferencing is supervised appropriately for the learner's age;
- consider my professional role and representation of the school when posting on social media and not refer to the school in a negative way (whether directly or indirectly);
- pass on any examples of Internet misuse or concerns to a senior member of staff or the Computing co-ordinator;
- post any supplied E-safety guidance appropriately;
- think carefully about what is stored on my laptop and ensure sensitive data is only stored on the school server or private area on the Learning Platform.

I agree that I will not visit Internet sites or make, post, download, upload or pass on: material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography);
- promoting discrimination of any kind;
- promoting racial or religious hatred;
- promoting illegal acts;
- breach any Local Authority/School policies, e.g. gambling;
- do anything which exposes children to danger;
- any other information which may be offensive to colleagues;
- forward chain letters;
- breach copyright law.

I accept that my use of the school and Local Authority Computing facilities may be monitored and the outcomes of the monitoring may be used.

Signed ..... **Print** ..... **Date** .....

Dovecotes Primary School
Laptop Agreement for Staff

This document is an agreement between both staff and school, and shall be binding for the duration employment at the school.

General

1. The laptop shall remain the property of the school.
2. The laptop shall be retained by staff in order to exercise their professional duties.
3. The laptop shall be returned to school upon a member of staff leaving school to either take up a post elsewhere or for long term leave (sick or maternity) and any additional saved data removed.
4. Staff are to take proper care of the laptop at all times.
5. Staff shall be responsible for the security of the laptop, ensuring it is in a lockable cupboard when unattended in school and ensuring all reasonable precautions are taken when transporting the laptop.
6. Any additional software installed on the laptops is to be correctly licensed.
7. All faults are to be reported to the Computing Co-ordinator and/or Computing technician.

Use

1. The laptop shall be available for use in school each day.
2. Staff shall be aware of the issues relating to access to Internet sites not relevant or appropriate to their professional duties.
3. Staff shall operate Internet access with due regard to school and Wolverhampton City Council policies.
4. Staff shall use the laptop in a responsible and professional manner.
5. Staff will be expected to use the laptop for:
    - Planning
    - Delivery of lesson
    - Record Keeping
    - Analysis of assessment
    - Target Setting
    - Accessing Learning Platform
    - Other professional duties

The school agrees to provide training for teachers in order to make effective use of their laptop.

I ..... agree to the terms and conditions above.

Signed .....

Laptop Serial Number: ..... Orange Tag number: .....
This laptop will be kept ***at home/in school** each night. **(Delete as appropriate)**

.....
L.Gould (Computing co-ordinator) signed on behalf of Dovecotes Primary School

Dovecotes Primary School
EYFS Parent and Pupil Internet/Social Media
Acceptable Use Policy

Computers and the use of the internet are a valuable resource for learners of all ages. Computing increasingly provides the focal point of educational content within the UK. The school's Computing policy sets out how the school intends to teach and use Computing to benefit its pupils' education. However, Dovecotes Primary School acknowledges that computers and the internet do have the potential for inappropriate use and access to undesirable material and that we have a duty of care to protect our pupils. The purpose of this agreement is to set out procedures which will minimise the misuse of the internet and Learning Platform at home, with parents, pupils and staff working together to achieve a safe and secure online experience.

Parent's Agreement

- I will know when my child is using the Internet at home and will monitor their usage.
- Online communication sent and received from school systems (or other networking sites) should not be considered private and I should inspect my child's messages.
- As a parent, I will ensure my child keeps to the above rules and that if he/she misuses online communications (or other public networking sites), their access may be withdrawn immediately.

As a parent/carer, I agree that I will set a good example in my own use of technology, including social media by:

- Demonstrating courtesy and respect for staff, other parents and pupils when comments are placed on social networking sites;
- Using appropriate language when discussing school;
- Addressing any issues or concerns regarding school, directly with the Headteacher, member of staff or governors rather than posting them on social media.

I agree that I will not:

- Use social network sites to make derogatory comments or post photographs which could bring the school into disrepute, including making comments about pupils, parents, the school staff, the senior leadership team, governors, local authority or the wider community;
- Post photographs or videos of other people's children on social network sites in order to keep all children safe, unless parental permission is given.

Pupil Name: _____ Class: _____

Parent Signature: _____ Print Name: _____

Date: _____

Dovecotes Primary School

AUP For learners in KS1

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret;
- talk to my teacher before using anything on the internet;
- only open pages which a responsible adult has said are OK;
- tell a responsible adult if anything makes me feel scared or uncomfortable;
- not give my mobile phone number to anyone who is not a friend in real life;
- not give personal information away (name, address and family and pets);
- not upload photographs of myself onto the internet;
- never agree to meet a stranger;
- only communicate with people I know in real life;
- tell my teacher if I get a nasty message through a computer or phone;
- not reply to any nasty message or anything which makes me feel uncomfortable;
- make sure all messages I send are polite;
- only communicate online with people I know or if my teacher agrees;
- only put something online that I would be happy to say to my teacher – nothing that may upset another child, teacher or adult.

I understand:

- Using computers safely can make everyone's learning more enjoyable;
- Anything I do on the computer may be seen by someone else;
- Anything I put online will have my name next to it.

Name _____

Date _____

Dovecotes Primary School

AUP For learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- Always keep passwords secure (safe/private combination of letters/numbers) and secret;
- Only visit sites which are appropriate to my work at the time;
- Work in collaboration with individuals or groups agreed by my teacher/responsible adult;
- Make sure I have permission from my teacher and subjects before taking photographs;
- Tell responsible adults immediately if anything makes me scared/uncomfortable online;
- Make sure all messages I send are respectful;
- Inform a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable or upset;
- Not reply to/forward nasty messages or anything that makes me feel uncomfortable;
- Not give my mobile phone number to anyone who I don't know or have not met;
- Only communicate online with people I know or approved by a responsible adult;
- Only use communication in school which has been provided by school;
- Only use school devices for my work and take any other personal devices to the office with an accompanying letter explaining why they are required in school;
- Only connect to the agreed school wireless broadband in school on school devices;
- Talk to a responsible adult before joining networking sites;
- Only put something online that I would be happy to say to my teacher – nothing that may upset another child, teacher or adult.
- Inform a responsible adult if anything on networking sites makes me feel uncomfortable;
- Always keep my personal details private (my name, family information, journey to school, my pets and hobbies are all examples of personal details);
- Always check with a responsible adult and parents before I upload photographs;
- Never meet an online friend without taking a responsible adult that I know with me.

I understand:

- Using computers safely can make everyone's learning more enjoyable;
- Anything I do may be seen by someone else and should have my name next to it;
- Most social networking sites have a minimum joining age (usually 13) and it is a criminal offence to give false information e.g. lie about my age or gender;
- Not everyone online is who they say they are;
- Once I post a message, picture or post online then it is completely out of my control;
- I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.

Name _____

Date _____

Dovecotes Primary School AUP

Parent and Pupil Internet/Social Media/Website

Computers and the use of the internet are a valuable resource for learners of all ages. The school's Computing policy sets out how the school intends to teach and use Computing to benefit its pupils' education. However, Dovecotes Primary School acknowledges that computers and the internet do have the potential for inappropriate use and access to undesirable material and that we have a duty of care to protect our pupils. The purpose of this agreement is to set out procedures which will minimise the misuse of the internet with parents, pupils and staff working together to achieve a safe and secure online experience.

Pupil's Agreement

When using the computer, I agree to the rules in the learners' AUP to keep me safe:

- Only visit sites which are appropriate to my work at the time;
- Tell responsible adults immediately if anything makes me scared/uncomfortable online;
- Make sure all messages I send are respectful;
- Inform a responsible adult if I receive anything that makes me feel uncomfortable or upset;
- Not reply to/forward nasty messages or anything that makes me feel uncomfortable;
- Only communicate online with people I know or approved by a responsible adult;
- Only use communication in school which has been provided by school;
- Talk to a responsible adult before joining networking sites and be aware that most social networking sites have a minimum joining age (usually 13);
- Only put something online that I would be happy to say to my teacher – nothing that may upset another child, teacher or adult.

Parents' Agreement

- I will know when my child is using the Internet at home and will monitor their usage.
- Online messages sent and received from school systems should not be considered private and as a parent I can inspect my child's online communication.
- As a parent I will ensure my child keeps to the above rules and that if he/she misuses online communications (or other public networking sites), their access may be withdrawn.

As a parent/carer I will set a good example, including on social media by:

- Demonstrating courtesy and respect for staff, other parents and pupils when comments are placed on social networking sites;
- Using appropriate language when discussing school;
- Addressing any issues or concerns regarding school, directly with the Headteacher, member of staff or governors rather than posting them on social media.

I agree that I will not:

- Use social network sites to make derogatory comments or post photographs which could bring the school into disrepute, including making comments about pupils, parents, the school staff, the senior leadership team, governors, local authority or the wider community;
- Post photographs or videos of other people's children on social network sites in order to keep all children safe, unless parental permission is given.

Parent Signature: _____ Print Name: _____
Pupil Signature: _____ Print Name: _____
Class: _____ Date: _____

Dovecotes Primary School
Photo and video consent form

We would be grateful if you would complete this form to give us permission to take photos/videos of your child and use these in our printed and online publicity.

I give Dovecotes Primary School permission to take photographs and/or video of my child.

I grant Dovecotes Primary School full rights to use the images resulting from the photography/ video filming, and any reproduction or adaptations of the images. This might include (but is not limited to), the right to use them in their printed and online publicity, social media, in training presentations and the Dovecotes YouTube Channel which **will be private** and **exclusive to Dovecotes' website.**

Name of child	
Class	
Name of parent/ guardian	
Signature of parent/ guardian	
Date	

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 E-Safety Policy Template and of the 360 degree safe E-Safety Self Review Tool:

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

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

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.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

'Keeping Children Safe in Education' 2019;

Early Years and Foundation Stage 2017;

'Working Together to Safeguard Children' 2018

Searching, Screening and Confiscation 2018

Education for a Connected World by the UK Council for Child Internet Safety, 2018

UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/ ThinkUKnow

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

Specialist help and support SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

Somerset - Questions for Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol