Online Safety Policy

Rationale

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to /loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- Inappropriate communication / contact with others, including strangers
- Cyberbullying
- The risk of radicalisation
- Access to unsuitable video /internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the offline world and it is essential that this online safety policy is used in conjunction with all other policies, in particular Anti-bullying, Equality, Teaching and Learning, PHSE, Health and Safety, Positive Behaviour, Allegations against Staff, Child Protection, Safeguarding, and Staff Code of Conduct.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues, in order to help young people (and their parents/ carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Monitoring and Review

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 or incidents that have taken place.

Agile Internet protection and filtering offers a higher standard than specified by the DfE requirements.

Agile provide a monthly Internet Summary Report to the Headteacher which can be requested and monitored by the Governing Body.

A log of reported incidents is kept by the Headteacher and is updated as appropriate.

Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of 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 the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Incidents arising out of this policy will be dealt with according to the school's Care and Control policy. The school will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety 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 IT Governor receiving information about online incidents and monitoring reports.

Headteacher and Senior Management Team:

- The Headteacher is responsible for ensuring safety (including online) of members of the school community
- The Headteacher is responsible for ensuring that the staff receive suitable CPD to enable them to carry out their online roles and to train other colleagues, as relevant
- The Headteacher receives reports of online incidents through the monthly Agile Internet Summary Report and updates a log of incidents to inform future online developments as required
- The Headteacher will remind parents that for safeguarding purposes, they should never take photographs or videos of children in school, other than their own, without the explicit consent of their parents
- Carole Ward is designated General Data Protection Officer and acts in accordance with GDPR regulations

Agile ICT act as Network Manager for Tavistock and ensure:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the online technical requirements outlined in any National Guidelines
- That users may only access the school's networks through a properly enforced password protection policy
- That the use of the network remote access is regularly monitored in order that any misuse or attempted misuse can be investigated

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of online matters and of the current school online policy and practices
- They have read, understood and signed the school's Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- Digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- Online issues are embedded in all aspects of the curriculum and other school activities
- Pupils (at the appropriate level) understand and follow the school online and acceptable use policy
- Pupils (at the appropriate level) have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- They are aware of online issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school 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 any unsuitable material that is found in internet searches

Designated Safeguarding Lead Joanne O'Connor and in her absence DDSL Claire Jamfrey are trained in online issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming
- Cyberbullying

Pupils (at an age-appropriate level and supported by teachers and/or parents):

- Are responsible for using the school ICT systems in accordance with the pupil acceptable use table (page 10), this is monitored by teachers. Should school be required to deliver virtual learning pupils would be expected to follow the acceptable use of the VLE under the guidance of their parents/carers

- Understand 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 school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyberbullying
- Should understand the importance of adopting good online 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online campaigns / literature.
Parents and carers will be responsible for:

- Supporting their children to follow the acceptable use of IT table (page 10)
- Accessing the school website / VLE (when applicable), online student / pupil records in accordance with the relevant school acceptable use guidance (page 10)

Community Users:

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements
Education – pupils (at an age-appropriate level)

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

Online Safety education will be provided in the following ways:

- A planned online programme should be provided as part of the ICT and PHSE curriculum and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key online messages should be reinforced as part of a planned programme of assemblies and curriculum activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil acceptable use and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of online risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, our website
- Reference to relevant online websites

Education & Training – Staff

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 training will be made available to staff. There is no statutory requirement for this to be done annually and at Tavistock it is completed on a 3 year cycle. An audit of the online training needs of all staff will be carried out regularly by Caroline Coleman, Senior Administrative Officer.

- All new staff should receive training/information as part of their induction programme ensuring that they fully understand the school online safety policy
- This online safety policy and its updates will be presented to and discussed by staff during INSET/staff meeting sessions
- The headteacher will provide updated advice / guidance / training as required

Training – Governors

Governors should take part in online training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / online / health and safety / child protection/ 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 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 online responsibilities:

- School ICT systems will be managed in ways that ensures that the school meets the online technical requirements outlined in any relevant Local Authority Online Policy and guidance
- There will be regular reviews and audits of online safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username
- The 'master / administrator' passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place (e.g. school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that

there has been a breach of security

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed practice is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed practice is in place regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school
- An agreed practice is in place regarding the installation of programs on school workstations / portable devices
- An agreed practice is in place regarding the use of removable media (e.g. memory sticks /CDs / DVDs) by users on school workstations / portable devices
- The school infrastructure and individual workstations are protected by up-to-date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Curriculum
Online should be a focus in all areas of the curriculum and staff should reinforce online messages in the use of ICT across the curriculum.

- 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online 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

Use of Digital and Video Images Photographic, Video
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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Pupil’s work can only be published with the permission of the pupil or parents/carers

General Data Protection Regulations

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018 which state 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

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

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: 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 need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and pupils or parents / carers (email, chat, 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 public chat / social networking programmes must not be used for these communications
- Whole class or group email addresses will be used at KS1 if required
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices other than provided by the school				x				x
Use of handheld devices e.g. PDAs, PSPs	x							x
Use of school network for personal purposes				x				x
Use of school email for personal emails				x				x
Use of chat rooms / facilities outside of the VLE				x				x
Use of instant messaging outside the VLE				x				x
Use of social networking sites				x				x
Use of blogs outside the school blog				x				x

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 certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Unacceptable
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			X
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation			X
	adult material that potentially breaches the integrity of the ethos of the school or brings the school into disrepute			X
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Agile and / or the school				X
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X
Creating or propagating computer viruses or other harmful files				X
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet			X	
Online gaming (educational)		X		
Online gaming (non educational)				X
Online gambling				X
Online shopping / commerce			X	
File sharing on the school network			X	
Use of social networking sites on the school network				X
Uploading of school events e.g. school plays on social networks				X
Use of video broadcasting e.g. YouTube for educational purposes		X		

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Such incidents will be dealt with in accordance with the school's policies particularly: Antibullying, Equality, Teaching and Learning, PHSE, Health and Safety, Care and Control, Allegations against Staff, Child Protection, Safeguarding, Staff Discipline and Online Safety policies.