



The Pathway Academy Trust

Online Safety Policy 2017

Contents

1. Creating an Online Safety Ethos
 2. Online Communication and Safer Use of Technology
 3. Social Media Policy
 4. Use of Personal Devices and Mobile Phones
 5. Policy Decisions
 6. Engagement Approaches
 7. Managing Information Systems
 8. Responding to Online Incidents and Safeguarding Concerns
- Appendix A

1. Creating an Online Safety Ethos

- **Aims and policy scope**
- TPAT believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- TPAT identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- TPAT identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.
- The purpose of the TPAT online safety policy is to:
 - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that TPAT schools are a safe and secure environment.
 - Safeguard and protect all members of the TPAT community online.
 - Raise awareness with all members of the TPAT community regarding the potential risks as well as benefits of technology.
 - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
 - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the directors, governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of TPAT (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding, Anti-Bullying, Behaviour, Data Security, Image Use, Acceptable Use Policies, Confidentiality, and relevant curriculum policies including computing and Personal Social and Health Education (PSHE).

1.2 Writing and reviewing the online safety policy

The Designated Safeguarding Leads (DSL) are:

CGPS: Ruth Doughty, Rachel Rodwell & Phil Jack

Safeguarding Governor: Priya Shorne

RIS: Nicole Caulfield, Emma Booker, Sue Garrard

Safeguarding Governor: Hits Patel

RJ: James Kendall, Emma Ellerington, Kerrie Ward

Safeguarding Governor: tbc

Policy approved by Directors of TPAT

Date: 12.12.17

The date for the next policy review is December 2018 2018

- The TPAT online safety policy has been written by the trust, involving staff, pupils and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.
- The policy has been approved and agreed by the Leadership Team and Directors.
- The schools have appointed Designated Safeguarding Leads as appropriate members of the leadership team and the online safety lead.
- This policy and its implementation will be reviewed by the Trust at least annually or sooner if required.

1.3 Key responsibilities for the community

1.3.1 The key responsibilities of the school leadership team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the trust community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network systems are actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- Monitor the online safety incidents to identify gaps/trends and use this data to update education response to reflect need.
- To report to the school leadership team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the school leadership to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.

- Ensuring that the use of the network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the IT infrastructure is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced.

1.3.5 The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

- Reading the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school website

- TPAT will ensure that information posted on the school websites meet the requirements as identified by the Department for Education (DfE).
- The contact details on the websites will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teachers will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The websites will comply with guidelines for publications including accessibility, respect for intellectual property rights, privacy policies and copyright.
- Pupils' work will be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online

- The school will ensure that all use of images and videos take place in accordance with other policies and procedures including Data Security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding records.
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Excessive social email use can interfere with teaching and learning and is not permitted during school work hours or whilst using school devices.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official videoconferencing and webcam use for educational purposes

- The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent will be obtained prior to children taking part in videoconferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.

2.5 Appropriate and safe classroom use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- Internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability:
 - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
 - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The schools will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The schools will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole- school requirement across the curriculum.
- The schools will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the TPAT community and exist in order to safeguard both the schools and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the TPAT community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the TPAT community.
- All members of the TPAT community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The schools will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.
- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the TPAT community on social media sites should be reported to the leadership teams and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding.
- Any breaches of TPAT policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2. Official use of social media

- Culverstone Green Primary School official social media channel is:
<https://www.facebook.com/Culverstone-Green-Primary-School-803036029765908/>
- Official use of social media sites by the schools will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and safeguarding.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.

- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from the Leadership Team.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of the schools will, where possible, be read and agreed by at least one other colleague.
- Official social media channels will link back to the school websites and/or Acceptable Use Policy to demonstrate that the account is official.
- The schools will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.
- If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils/parents received on personal social media accounts will be reported to the Designated Safeguarding Lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with TPAT policies and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role.
- Members of staff are encouraged not to identify themselves as employees of TPAT or the individual schools on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who *follow/like* the school on social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

3.4 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially will disclose their official role but always make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially will sign the school social media Acceptable Use Policy.

3.5 Pupil use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and strong passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13; therefore they will not create accounts within schools specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the TPAT community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies.
- TPAT recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools.

4.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- Electronic devices of all kinds that are brought on site are the responsibility of the user at all times. The schools accept no responsibility for the loss, theft or damage of such items. Nor will the schools accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school sites such as changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required.
- All members of TPAT community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of TPAT community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen.

Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

- All members of the TPAT community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school's policies.
- School mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the Acceptable Use Policy.
- Pupil's personal mobile phones and personal devices are not allowed in school other than in exceptional circumstances when they will be kept in a secure place in the school office to be collected at the end of the school day.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

4.5 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches TPAT policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.

- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following TPAT policy.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the TPAT Acceptable Use Policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- TPAT is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school Leadership Teams will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The schools will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- The schools will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The schools will audit technology use to establish if the online safety (e-Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the Leadership Teams.

5.2 Authorising internet access

- The schools will maintain a current record of all staff and pupils who are granted access to devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as with children with special education needs) the schools will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be established and embedded throughout the schools, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupil input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and internet use will be monitored.
- Online safety (e-Safety) will be included in the PSHE and Computing programmes of study, covering both safe school and home use.
- Acceptable use expectations and posters will be posted in all rooms with internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support internal online safety (e-Safety) education approaches.

6.2 Engagement and education of children and young people considered to be vulnerable

- TPAT is aware that some children may be considered to be more vulnerable online due to a range of factors.
- TPAT will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

6.3 Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Members of staff with a responsibility for managing filtering systems or who monitor IT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The schools will highlight useful online tools which staff should use according to the age and ability of the pupils.

6.4 Engagement and education of parents and carers

- TPAT recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the online safety (e-Safety) policy and expectations in newsletters, letters and on the school website.

- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Full information regarding the approach to data protection and information governance can be found in the Data Security policy.

7.2 Security and Management of Information Systems

- The security of information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing manager and network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

7.3 Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.

- From year 3, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff to use strong passwords for access into our system.
- We require staff to change their passwords regularly.

7.4 Filtering and Monitoring

- The directors will ensure that the schools have age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- The internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The schools use educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our pupils.
- The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The schools will work with the broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The schools will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

7.5 Management of applications (apps) used to record children's progress

- The Headteachers are ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

- Parents will be informed of expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- Complaints about internet misuse will be dealt with under the school complaints procedures.
- Complaints about online/cyber bullying will be dealt with under TPAT anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school complaints procedures.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the community.
- The schools will manage online safety (e-Safety) incidents in accordance with the discipline/behaviour policy where appropriate.
- The schools will inform parents/carers of any incidents of concern as and when required.
- After any investigations are completed, the schools will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the schools will contact the Education Safeguards Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- If the schools are unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.
- Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

Online Safety (e-Safety) Contacts and References

Kent Support and Guidance

Kent County Councils Education Safeguards Team:

www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

Kent Online Safety Support for Education Settings

- 1 Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- 2 Ashley Assiter, e-Safety Development Officer
- 3 esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police:

www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kent e-Safety Blog: www.kentesafety.wordpress.com

EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: <http://www.mariecollinsfoundation.org.uk/>

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: <https://360safe.org.uk/>

Online Compass (Self review tool for other settings): <http://www.onlinecompass.org.uk/>