Kenningtons

Primary Academy

Online Safety Policy

Contents

Development of this Policy

This Online Safety policy has been developed by an Online Safety Strategic group made up of:

- Headteacher- Jo Sawtell- Haynes
- Online Safety Officer / Coordinator- Leea Chatfield
- Tracey Dole- Pastoral Manager
- Alana Branch- SENCO
- Claire Kavanagh- Senior Leader
- Eleanor Maguire- Class teacher

Our policy sets out the way our school will:

- Educate all members of our school community on their rights and responsibilities with the use of technology
- Build both an infrastructure and culture of online Safety
- Work to empower the school community to use the Internet as an essential tool for life-long learning.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of student pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the, but is linked to membership of the school.

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

Roles and Responsibilities

Role	Responsibility
Governors	Approve and review the Online Safety Policy and for reviewing the effectiveness of the policy.
Headteacher	Has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator. Follows the correct procedures in the event of a serious online safety allegation being made against a member of staff. Ensure that there is a system in place to monitor online safety. Ensure that all staff receive suitable CPD to carry out any online safety issues. Inform the Thurrock Council about any serious Online Safety issues. Annual monitoring online presence, this will result in notifying parents.
Online Safety Coordinator	Leads the Online Safety Group Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. Provides training and advice for staff

	Liaises with the Local Authority / relevant body LADO- 01375652921 Liaises with school technical staff Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments Liaise with safeguarding governor (if needed) Reports regularly to Senior Leadership Team
Technical staff	That the school's technical infrastructure is secure and is not open to misuse or malicious attack That the school meets required online safety technical requirements and any Local Authority 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant. That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction. That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and support staff	They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices They have read, understood and signed the Staff Acceptable Use Policy/ Agreement (AUP) They report any suspected misuse or problem to the Headteacher for investigation / action / sanction. All digital communications with students/ parents / carers should be on a professional level and only carried out using official school systems. Online safety issues are embedded in all aspects of the curriculum and other activities Students understand and follow the Online Safety Policy and acceptable use policies. They monitor the use of digital technologies, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices In lessons, where internet use is pre-planned students 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	Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from: • Sharing of personal data • Access to illegal / inappropriate materials

	• Inappropriate on-line contact with adults / strangers • Potential or actual incidents of grooming • Cyber-bullying
Online Safety Group	The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body. Members of the Online Safety Group will assist the Online Safety Coordinator with: • The production / review / monitoring of the school Online Safety Policy / documents. • Monitoring network / internet / incident logs • Consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
Students	Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement. Read and sign an Acceptable Usage Agreement and follow the guidance. To become informed of the procedures in place to protect them. Participate in Online Safety Activities Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions

	out of school, if related to their membership of the school.
Parents/Carers	Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • Digital and video images taken at school events. • Maintaining responsible standards when using social media to discuss school issues.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision.

The school has to ensure there is progression throughout the school linked to online safety. These lessons take place through discrete lessons and across the curriculum for all children. Key online safety messages are reinforced through:

- Planned lesson within computing and PSHE.
- Assemblies
- Safer Internet Day
- Outside agencies

- Students 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.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, and web site,
- Newsletters- every three weeks, the newsletter provides top tips and advice for parents and carers.
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

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

- Annual online safety training will be carried out each year.
- All new staff should receive online safety training as part of their induction programme.

Training – Governors / Directors

Governors should take part in online safety training sessions. They will participate 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 safety responsibilities:

The school ensures that working with their technical support the following guidelines are used:

- The School ICT systems are managed in ways that ensure that the school meets E-Safety technical requirements
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
- The downloading of executable files by users
- The extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
- The installing programs on school devices unless permission is given by the technical support provider or Computing Lead
- The use of removable media (e.g. memory sticks) by users on school devices
- The installation of up to date virus software

Access to the school network and Internet will be controlled with regard to: -

- Users having clearly defined access rights to school ICT systems through group policies
- Users being provided with a username
- Staff users being made aware that they are responsible for the security of their username and password, which they are required to change regularly. They must not allow other users to access the systems using their log on details
- The 'master/administrator' passwords are available to the Head Teacher and kept in a locked filing cabinet
- Users must immediately report any suspicion or evidence that there has been a breach of security
- Filtering ensures that children are only able to access appropriate website

Use of digital and video images

Staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press.
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment, the personal equipment of staff should not be used for such purposes. In certain circumstances, and where Head Teacher has given permission, personal devices may be used for education purposes only.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Student's work can only be published with the permission of the student and parents or carers.

Data Protection (see Data Protection Policy)

Communications

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

	Staff & other adults			Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	☐							✔
Use of mobile phones in lessons			☐					✔
Use of mobile phones in social time	✔							
Taking photos on mobile phones / cameras			✔					✔
Taking photos on school devices	✔				✔			
Use of other mobile devices e.g. tablets, gaming devices	✔							✔
Use of personal email addresses in school, or on school / academy network	✔							✔
Use of school / academy email for personal emails	✔							✔
Use of messaging apps*	✔							✔
Use of social media*			✔					✔

Use of blogs *		✔		✔

*Used at appropriate times and in an appropriate manner.

Then using communication technologies the school / academy considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school / policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs etc.) must be professional in tone and content. Communication with parents, must go through the enquires or admin email addresses (enquiries@kenningtons.thurrock.sch.uk or admin@kenningtons.thurrock.sch.uk).
- Whole class / group email addresses may be used at KS1, while students at KS2 and above will be provided with individual school email addresses for educational use (where needed).
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website.

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 and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published
- Training is provided for all staff.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to students, 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

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

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts
- A code of behaviour for users of the accounts, including:
- Reporting and dealing with any abuse and or misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

Unsuitable / inappropriate activities

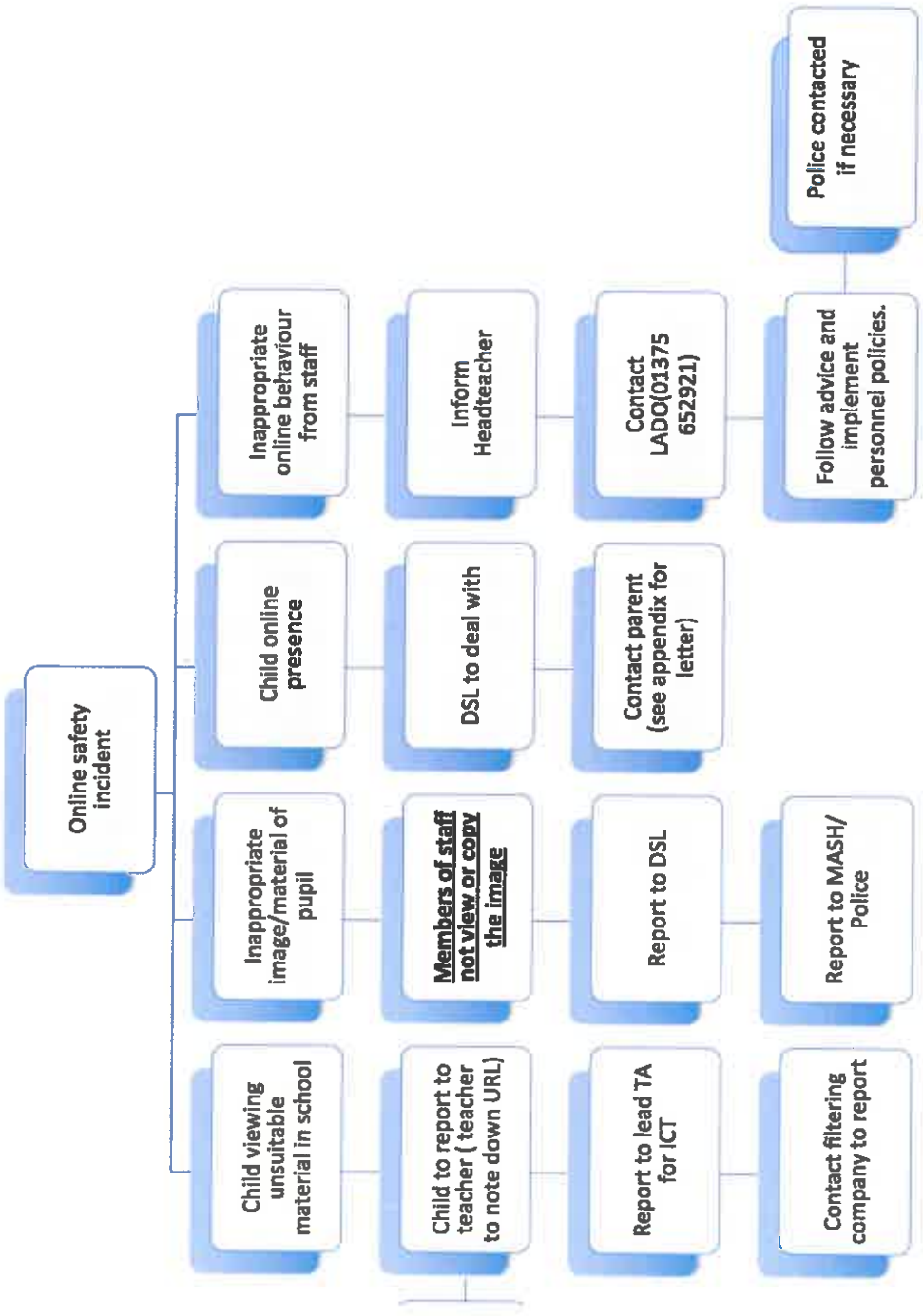
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities. 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:	Pornography of any kind (Contrary to the Criminal Justice and Immigration Act 2008, Sexual Offences Act 2003, contrary to the Public Order Act 1986					X
	Promotion of any kind of discrimination- including criminally racist material, promotion if extremism or terrorism				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	

Online Safety Incidents

If an incident takes place in school, follow the flow chart to ensure the appropriate action is taken.



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
    - Promotion of terrorism or extremism
    - Other criminal conduct, activity or materials
    - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding

purposes. The completed recordings should be retained by the group for evidence and reference purposes.

Policy Review

The Governing Body of our school is responsible for ensuring the annual review of this policy.

Signed on behalf of the Governing Body: Sarah Leyes (CHAIR OF GOVERNORS)

Date adopted: 15/03/18

Date for review: MARCH 2019

Appendices

Contents

Student Acceptable Use Agreement

School Policy

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

This Acceptable Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- Keep my username safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- Be aware of "stranger danger", when I am communicating on-line.
- Do not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- Report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Be considerate and respectful of others
- Use the computer/internet for the purpose intended.
- Only do things on devices that you are told to do.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

I have read and understand the above and agree to follow these guidelines

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Student Acceptable Use Policy Agreement (Foundation / KS1)-

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen

Signed (child): .....

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate

awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

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

KS2 - I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)- I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school.

- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school / academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Technician Acceptable Use Policy Agreement Template

The school ICT Technician or person with administration rights is placed in an exceptional position of trust. Many of the duties that the Head Teacher expects these people to complete could be against the Staff Acceptable User Policy of the school. This document is not a job description but an addition to the Staff Acceptable User Policy that allows the ICT technician to fulfill these duties. Schools should customise this document to fit their needs.

Areas of concern are that:

- Files may be created, imported or processed by staff and pupils and stored on the school's servers or other storage systems (e.g. USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.
- User accounts will need to be created and serviced meaning that there may be access to these accounts by the ICT technician.
- Through work within the school's administration network the ICT Technician may be placed in the position of assisting in the processing of confidential information including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.
- The ICT technicians through specific user names and password have control, (sometimes through remote workstations) to the schools network. In the past there have been examples where these powers have been abused.

Because of these areas of concern the ICT Technician should:

- Be responsible for monitoring the school's network.
- Be given permission to access other user's files.
- Protect the users by maintaining a filter for the school.
- Monitor the internet use of users within the school.
- Be aware of the laws relating to the use of computers especially those around Data Protection, Copyright and those referred to in the school's Online Safety Policy and AUPs.
- Make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them.
- Have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- Receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information.
- Have an agreed procedure for managing the internet filter. This should include a log of decisions made.
- Have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet.
- Have agreed procedures for reporting incidents.
- Log any incidents including minor ones that are quickly resolved.
- Be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise (e.g. never open websites that are suspected of having inappropriate material unless others are present).

- Have frequent meetings with their line manger to report on any issues or trends.

As an ICT Technician (or a person who has similar responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the appropriate member of Senior Management.

Name: _____

Signed: _____

Senior Member of Staff:_____

Date: _____