Lakeside Primary School

Online Safety Policy

Policy Status and Review

Date:	**November 2024**
Review Date:	**October 2025**
Signed by Governor:	**Les Powell**
Date Signed:	**29th November 2024**

1. Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body	
The implementation of this Online Safety policy will be monitored by the:	Online Safety Leader, DSL/DDSL, Headteacher & Senior Leadership Team
Monitoring will take place at regular intervals:	Once a term.
Governing Body will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	Once every Governors meeting.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	Ongoing to meet the ever changing role of technology and the needs for home learning. April 2023
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	Staffs Tech (support), Safeguarding Officer, Police.

The school will monitor the impact of the policy using:

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

2. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

3. Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports. In accordance with KCSiE September 2024, Governors should ensure they have had training on an annual basis about online safety.

A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Headteacher and Senior Leaders:

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

Online Safety Coordinator:

- 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 MAT / relevant body / Liaise with 'Staffs Tech'
- Liaises with school technical staff
- Receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- Meets with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

- attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

Network Manager / 'Staffs Tech' are the managed service provider/ Technical staff:

The Network Manager / Technical Staff / Co-ordinator for Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required Online Safety technical requirements and any MAT / other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering and monitoring policy (SENSO), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 /Senior Leader / Online Safety co-ordinator and action / sanction can be put in place.
- that monitoring software / systems are implemented and updated as agreed in school policies.

4. Teaching and Support Staff

All staff are responsible for ensuring that:

- they have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem using CPOMS (Online Safety file), to the Headteacher / Online Safety co-ordinator
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety and acceptable use policies
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils will 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.
- Ask for clarification if they are unsure about any aspect of the school policy
- Plan and teach the Online Safety Curriculum, which will be identified on long term and medium term planning.

- Ensure that school devices used in school or at home that all behaviour on the device should conform to professional standards and practice.
- Ensure that school devices are not used by family members

5. Child Protection / Safeguarding Designated Person / Officer

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

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

6. Parents / Carers / Families

Parents / Carers / Families 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
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices in the school

7. Education – Pupils

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

A planned Online Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorials
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

8. Education – pupils using IPads (no pupil IPads currently in use)

To ensure the safety of the pupils when using iPads, we triangulate our practice to include the robust teaching of our online safety curriculum, the children having a secure understanding of how to report incidents and constant supervision of their use alongside the filtering system used for the Internet in school.

When using the iPads, staff will (as far as possible & in keeping with the computing and online safety curriculum) use the Google classroom and school website as a basis for their teaching. This will ensure the children will only visit pages that the teacher has already monitored and ensured to be safe and appropriate.

9. Education – parents / carers

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

- Curriculum activities
- Letters, newsletters, web site, social media
- Online Safety family workshops
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

10. Education – The Wider Community

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

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

11. Education & Training – Staff / Volunteers

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

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced.

- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.
- The Online Safety Coordinator will receive regular updates by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Remote education

Remote education is included in our safeguarding considerations please consult our remote learning policy for more information.

Training – Governors

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

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

12. Technical – infrastructure / equipment, filtering and monitoring

Staffs Tech is the managed service provider and are aware of the school Online Safety policy.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Most users are responsible for the security of their username and password. Teachers and Teaching staff will manage passwords for pupils where appropriate.
- The master passwords are available upon request from Staffs Tech.
- The MAT Business Manager / Senior Operational offices Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Content is monitored using SENSO monitoring software.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach.

- Appropriate security measures are in place (Staffs Tech) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed system is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. This is regularly monitored. Students or guests have a user name and password set by Staffs Tech so they can access our system to support their teaching and so staff do not share their N Drives.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. This means that personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

13. Use of digital and video images

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

14. Data Protection – related to GDPR policy - see separate policy too

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school / academy must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out, when appropriate.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- Have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Expected to change their school passwords at least once a term.

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

- The data must be encrypted and password protected.
- The device must offer approved virus and malware checking software.

- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

15. Communications

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- 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 pupils or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1 & KS2 for educational use.
- Pupils are taught about Online Safety issues through the curriculum, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

16. Mobile Technologies

- All Mobile Technology used in school will be owned directly by the school and therefore the users will be subject to acceptable user agreements and the devices will be monitored in accordance with this policy.
- No personal devices for pupils should be brought into classrooms or the school grounds or used for educational purposes.
- Children are not allowed to bring in or wear smart devices or watches that have; internet access, access to any internet or social media based apps or the facility to take photographic or video images. Any devices with these accesses will be removed and kept in a secure locked cupboard before being returned to a person with parental responsibility. Children who bring in mobile/smart phones to ensure their safety before or after school, are required to bring them straight to the school office, where they will be locked in a secure cupboard for all school hours.
- Staff personal devices including smartwatches and phones should be set to do not disturb or silent. Phones should be kept out of sight of children and only used during breaks from the classroom, preferably in the staff room or any empty classroom.

17.Social Media - Protecting Professional Identity

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk. School staff should ensure that:
- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

School social media accounts:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts –

involving at least two members of staff

- A code of behaviour for users of the accounts, including:

-Systems for reporting and dealing with abuse and misuse

-Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

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

Monitoring of Public Social Media

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

18. Responding to incidents of misuse

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

• **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

19. Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer reporting systems attached below.

Reporting Incident Flowchart

20. 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.
    - Police involvement and/or action
- If content being reviewed includes images of **Child abuse,** then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
- All staff to report any online safety issues using CPOMS, recording in the Online Safety file.

Signed by (SLT):  Neil Probert

Date: 29.11.2024

Date for review: October 2025

21. Appendices

22. Glossary of Terms

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

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

23. STAFF ACCEPTABLE USE AGREEMENT

Introduction

This policy is designed to enable acceptable use for staff and governors.

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Head Teacher/Online safety lead.

Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.

No personal equipment should be connected to or used with the School's ICT systems. Users must not try to install any software on the ICT systems without permission from the Head Teacher/Online safety lead. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

the Head Teacher/School Business Manager are responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

Network access and security

All users of the ICT systems at the school must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the SLT for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Head Teacher/Online safety lead as soon as possible.

Users should only access areas of the school's computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

School Email

Where email is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this acceptable use policy. The school's email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address. Communication with our families will be professional in tone and manner.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.
- 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 or password protection.
- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.

- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked 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.

Internet Access

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use.

The school's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Head Teacher/Online safety lead.

Staff must not therefore access from the school's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the school and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the school);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the school may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring

records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital cameras

The school encourages the use of digital cameras and video equipment; however, staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press will only include pupils first names.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones.
- All photos should be downloaded to the school network
- The use of personal mobile phones for taking photos of pupils is not permitted, a school phone is provided for this purpose. Photos are immediately downloaded and then deleted from the phone

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Mobile Phones

Mobile phones are permitted in school, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard.
- Personal mobile phone cameras are not to be used on school trips. The school provides a trip phone/Ipad for this purpose.
- All phone contact with parents regarding school issues will be through the schools' phones. Personal mobile numbers should not be given to parents at the school.

Social networking

The school has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.

- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the school's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via the officially recognised school site and with the permission of the Head Teacher or the Deputy Head Teacher.
- Members of staff will notify the Head Teacher/Online safety lead 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 in the school/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).

Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by SENSO. SLT and the Online safety lead to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Head Teacher/Online safety lead considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Staff Conduct Agreement

We acknowledge that practitioners will use digital technologies in their personal and social lives so we require them to sign the following Professional Conduct Agreement to ensure clear boundaries between their home and professional roles.

I agree that through my recreational use of social networking sites or other online technologies that I will:

- not bring Mercia Primary Academy Trust into disrepute;
- observe confidentiality and refrain from discussing any issues relating to work;
- not share or post in an open forum, any information that I would not want children, parents/carers or colleagues to view;
- set privacy settings to block unauthorised access to my social networking page and to restrict those who are able to receive updates;
- keep my professional and personal life separate and not accept children and parents/carers as 'friends';
- consider how my social conduct may be perceived by others and how this could affect my own reputation and that of the Mercia Primary Academy Trust;
- either avoid using a profile photograph or ensure it is an image I would be happy to share with anyone;
- report any known breaches of the above;

I understand I am in a position of trust and my actions outside of my professional environment could be misinterpreted by others, and I am conscious of this when sharing information publicly with others.

Name: _____ Signature: _____

Date: ___/___/___

Setting's Social Media Conduct Agreement

We require staff to sign and agree to follow the Conduct Agreement for using Mercia Primary Academy Trust social media communication platforms to ensure clear boundaries between Mercia Primary Academy Trust and home are followed.

Social Media platform: _____

I agree to:

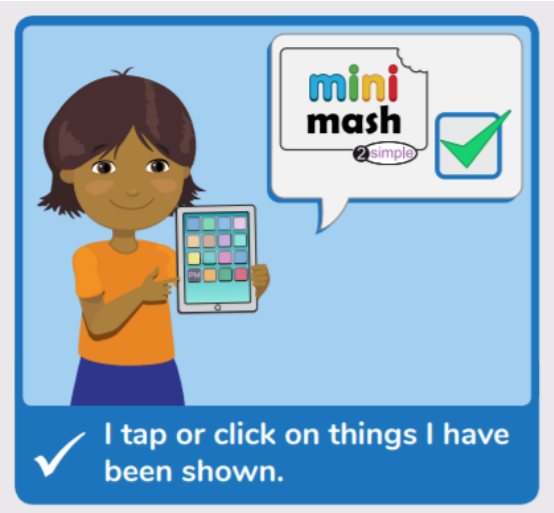
- not bring Mercia Primary Academy Trust into disrepute by following their social media policy;
- observe confidentiality by not discussing other children, parents or practitioners;
- not share, tag, post or copy any information from Mercia Primary Academy Trust social media platform without prior permission from the 'management';
- keep my professional and personal life separate and not accept children/ parents/carers as 'friends' on my personal page;
- consider how my social conduct may be perceived by others and how this could affect my own reputation and that of Mercia Primary Academy Trust;
- report any known breaches of the above to the designated person for safeguarding Mercia Primary Academy Trust and named social media administrator for social media;
- I understand I am in a position of trust and my actions could be misinterpreted by others and I am conscious of this when sharing information with others on the social media platform site belonging to Mercia Primary Academy Trust.

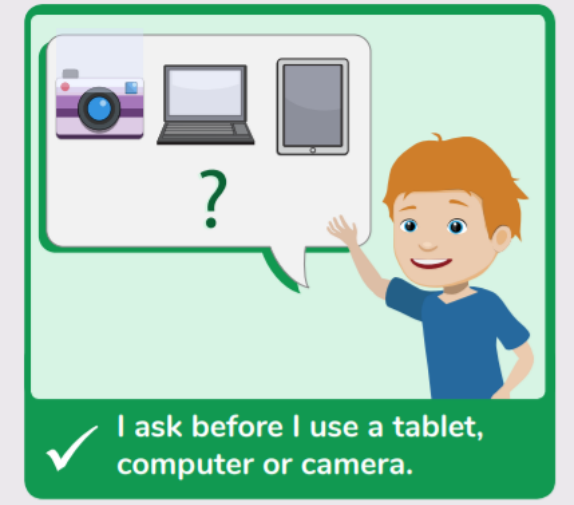
Name: _____ Signature: _____

Date: ____/____/____

Pupil Acceptable Use Policy Agreement
Early Years

NURSERY



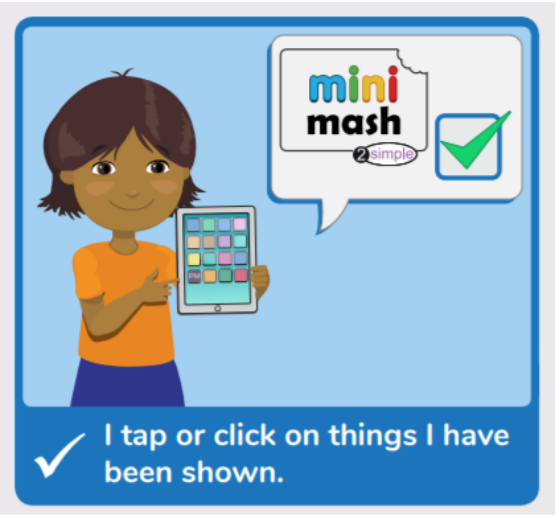


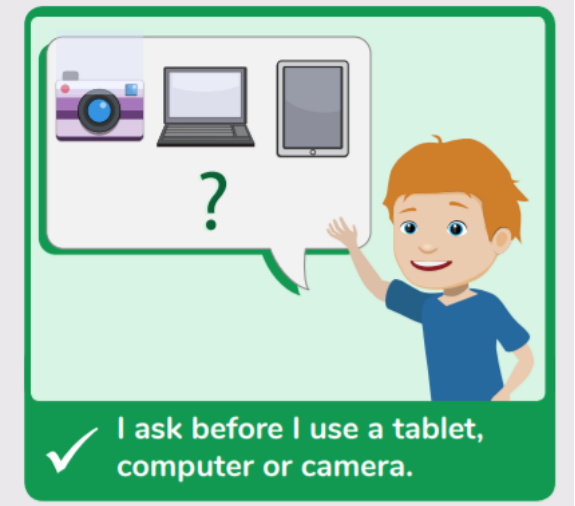
My name: ……

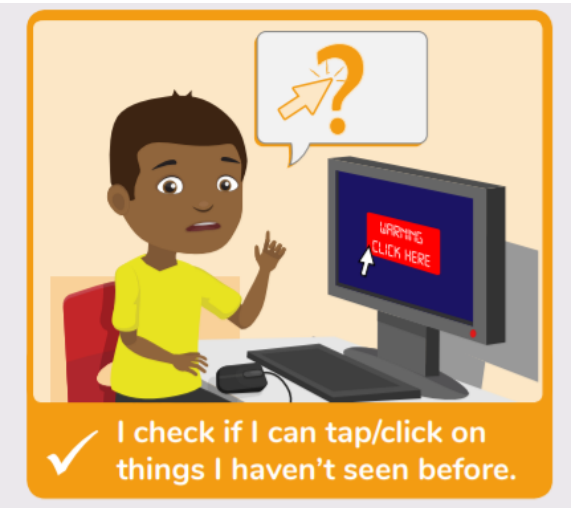
Date: ……

Pupil Acceptable Use Policy Agreement
Early Years

RECEPTION







My name: ……

Date: ……

Pupil Acceptable Use Policy Agreement
Key Stage 1

YEAR 1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I **KNOW** people online aren't always who they say they are
- I don't keep ~~**SECRETS**~~ or do **DARES AND CHALLENGES** just because someone tells me I have to
- I am **KIND** and polite to everyone

Signed (child): ……

Date: ……

Pupil Acceptable Use Policy Agreement
Key Stage 1

YEAR 2

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I **KNOW** people online aren't always who they say they are
- I don't keep ~~**SECRETS**~~ or do **DARES AND CHALLENGES** just because someone tells me I have to
- I am **KIND** and polite to everyone

Signed (child): ……

Date: ……

Pupil Acceptable Use Policy Agreement Key Stage 2

YEAR 3

- I will only access computing equipment when a trusted adult has given me permission and is present – at home or at school.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others. I will also make sure my password is strong and difficult to guess.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will be careful with what I click on online I won't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as Google Classroom. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- I will only communicate and collaborate online with people I already know and have met in real life or that a trusted adult knows about.
- I know new online friends might not be who they say they are and I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. And know when to say no online.

- Before I share, post or reply to anything online, I will T.H.I.N.K.

  T = Is it true?
  H = Is it Helpful?
  I = Is it Inspiring?
  N = Is it Necessary?
  K = Is it Kind?
- I understand that if I behave negatively whilst using technology towards other members of the school, my family will be informed and appropriate actions taken.

My name: ……
Date: ……

Pupil Acceptable Use Policy Agreement Key Stage 2

YEAR 4

- I will only access computing equipment when a trusted adult has given me permission and is present – at home or at school.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others. I will also make sure my password is strong and difficult to guess.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will be careful with what I click on online I won't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as Google Classroom. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- I will only communicate and collaborate online with people I already know and have met in real life or that a trusted adult knows about.
- I know new online friends might not be who they say they are and I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. And know when to say no online.

- Before I share, post or reply to anything online, I will T.H.I.N.K.

  T = Is it true?
  H = Is it Helpful?
  I = Is it Inspiring?
  N = Is it Necessary?
  K = Is it Kind?
- I understand that if I behave negatively whilst using technology towards other members of the school, my family will be informed and appropriate actions taken.

My name: ……
Date: ……

Pupil Acceptable Use Policy Agreement
Key Stage 2

YEAR 5

- I will only access computing equipment when a trusted adult has given me permission and is present – at home or at school.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others. I will also make sure my password is strong and difficult to guess.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will be careful with what I click on online I won't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as Google Classroom. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- I will only communicate and collaborate online with people I already know and have met in real life or that a trusted adult knows about.
- I know new online friends might not be who they say they are and I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. And know when to say no online.

- Before I share, post or reply to anything online, I will T.H.I.N.K.

  T = Is it true?
  H = Is it Helpful?
  I = Is it Inspiring?
  N = Is it Necessary?
  K = Is it Kind?
- I understand that if I behave negatively whilst using technology towards other members of the school, my family will be informed and appropriate actions taken.

My name: ……

Date: ……

Pupil Acceptable Use Policy Agreement
Key Stage 2

YEAR 6

- I will only access computing equipment when a trusted adult has given me permission and is present – at home or at school.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others. I will also make sure my password is strong and difficult to guess.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will be careful with what I click on online I won't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as Google Classroom. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- I will only communicate and collaborate online with people I already know and have met in real life or that a trusted adult knows about.
- I know new online friends might not be who they say they are and I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. And know when to say no online.

- Before I share, post or reply to anything online, I will T.H.I.N.K.

  T = Is it true?
  H = Is it Helpful?
  I = Is it Inspiring?
  N = Is it Necessary?
  K = Is it Kind?
- I understand that if I behave negatively whilst using technology towards other members of the school, my family will be informed and appropriate actions taken.

My name: ……
Date: ……

24. Reporting Incident Flowchart