E-Safety & Acceptable Use Policy

Review Programme:	
Policy adopted:	**Summer 2023**
Date for next review:	**Summer 2025**
Signed – Headteacher:	**L. Lee**
Date:	**May 2023**

What we do

At Sketchley Hill Primary School, we encourage pupils and staff to use technology to support teaching and learning, including access to the Internet. We also encourage and continue to explore ways of using technology to better streamline and improve our administration tasks. This E-Safety Policy for Sketchley Hill Primary School is designed to help to ensure safe and appropriate access and usage for all digital technologies across the school community.

For the purpose of this policy, digital technologies are defined as electronic tools, systems, devices and resources that generate, store or process data that can include, but are not restricted, to the following:

- Computers
- Laptops
- Websites
- Email
- Social media
- Mobile phones
- Tablets
- Blogs
- Podcasts
- Downloads
- Forums

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but are 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 as well as associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Why do we have an E-Safety Policy?

With the ever-increasing manner in the way technology is being used in education, it is paramount that as educators we have in place policies and strategies that help us to keep both staff and pupils safe. We have highly functional school-based and personal devices that give us access to powerful digital tools wherever we go. The Internet has the capacity to instantly connect us to content and to each other, but, due to its vast nature and relative immaturity as a medium, also presents unprecedented levels of risk to young people. Some of the dangers pupils may face include:

- Access to illegal, harmful or inappropriate content
- Access to content that promotes extremism and/or radicalisation
- Losing control over personal information/images
- The risk of being groomed by those with whom they make contact, exposing them to physical and sexual risk
- Exposure to, or engagement in cyber-bullying
- An over-reliance on unreliable sources of information and an inability to evaluate the quality accuracy and relevance of information on the Internet

Other school policies

This policy should be read in conjunction with other relevant school policies:

- Acceptable Use Agreements for Adults
- Acceptable Use Agreement for Pupils

- Keeping Children Safe in Education Policy
- Bring your own device Policy for Staff
- Bring your own device Policy for Governors
- Child Protection Policy
- Whole School Positive Behaviour Policy
- Anti-Bullying Policy
- PSHE Policy
- Staff Code of Conduct
- UK-GDPR Policy

Legal frameworks

It is the user's responsibility to ensure they are compliant and work within all UK and E.U. applicable legislation in regards to the safe and legal use of ICT in schools. This includes but is not limited to the following:

- The Sexual Offences Act 2003
- The Racial and Religious Hatred Act 2006
- The Computer Misuse Act 1990
- The Police and Justice Act 2006
- Communications Act 2003
- Data Protection Act 1998
- Malicious Communications Act 1988
- Copyright, Design and Patents Act 1988
- Public Order Act 1986
- Protection of Children Act 1978
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997
- The Regulation of Investigatory Powers Act 2000 (RIP)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011

Governor responsibilities

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The school's E-Safety Governor will monitor compliance with this policy by:

- Holding meetings with the E-Safety Co-ordinator/Officer
- Attending e-safety group meetings
- Monitoring of e-safety incident logs
- On-line safety and associated issues including filtering and monitoring in accordance with DfE monitoring standards.
- Reporting to relevant meeting

School leadership and management responsibilities

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Lead. 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 e-safety allegation being made against a member of staff. They are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues as relevant.

The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also to support those colleagues who take on important monitoring roles.

At Sketchley Hill Primary School we employ the filtering and monitoring systems recommended to us and installed by Primary World. We use Sonic Wall as our primary filtering software alongside ESET Anti-virus. This trusted and widely used filtering software complies to schools' standards and mitigates the risks of our children's online safety. The school's filtering system employs a continuously updated series of keywords and watchwords to filter the content of the internet from any of the machines within the school system. This complies with the new requirements outlined in KCSIE 2023.

The Designated Safeguarding Lead (DSL) responsibilities

Details of the school's Designated Safeguarding Lead (DSL) are set out in our Child Protection and Keeping Children Safe in Education Policy.
The DSL takes lead responsibility for e-safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any e-safety issues or incidents.
- The appropriateness of any filtering and monitoring systems to be informed by the risk assessment required by the Prevent Duty as required by KCSiE 2023 paragraph138 to147.
- Ensuring that any e-safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy.
- Updating and delivering staff training on e-safety.
- Liaising with other agencies and/or external services if necessary.
- Working with the Computing Lead to personalise the online safety curriculum in meeting the needs of our pupils.

Teaching and support staff responsibilities

All staff shall make themselves aware of the content of this policy and attend relevant e-safety training. Staff shall be responsible for contributing to the positive re-enforcement of e-safe behaviours through their day-to-day interaction with pupils and technology. Staff should ensure that e-safety issues are embedded in the curriculum and that pupils are following the school's terms on acceptable use.

It is the responsibility of teaching staff to ensure that the 4 C's (Content, Contact, Conduct and Commerce) is taught within the curriculum. This is included within, but not confined to, the PSHE and Computing curriculum.

Staff should act as good role models in their use of ICT, the Internet and mobile devices. Staff should report any misuse or problem to the DSL/DDSL for investigation and implement actions required of them. For any incidents of cyber-bullying, staff are to ensure that these are dealt with appropriately in line with the school's Positive Behaviour Policy.
Where personal devices are allowed, all teaching staff shall ensure that pupils' use of these devices is for legitimate educational purposes and not for texting, accessing social networking sites or recording audio, video or still imagery without permission.

All our staff have 'an understanding of the expectations, applicable to their roles and responsibilities in relation to filtering and monitoring' of ICT systems and regular monitoring of school's equipment and networks. All members of staff are provided with a school email address. Electronic communications with students, parents/carers and other professionals will only take place via work-approved communication channels e.g. via a school-provided email address or telephone number. Staff are advised to ensure that business correspondence is received to and sent from the school email address. This is to protect staff's privacy and ensure that school business is kept separate from private correspondence.

Parents' and carers' responsibilities

Parents and carers may have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's online experiences. Parents/carers can often underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and can be unsure about what they should do about it.
At Sketchley Hill Primary School, we will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, our website and other digital communications.
- Parents evenings.
- Family workshops in e-safety, so that parents/carers and children can together gain a better understanding of these issues.

Parents/Carers are expected to notify the school of any concerns or queries regarding this policy and ensure that their child has read, understood and agreed to the terms on acceptable use.

System management responsibilities

The school, in conjunction with their ICT support provider, will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that procedures set out within this policy are implemented:

- There will be regular reviews and audits of the safety and security of ICT systems.
- All users will have clearly defined access rights to the ICT systems of the school. This will be defined and accountable by the respective ICT lead/co-ordinator(s).
- Users will be made responsible for the security of their username and password; must not allow other users to access the systems using their login details; and must immediately report any suspicion or evidence that there has been a breach of security to the school's Data Protection Officer.

The administrator passwords for the ICT system must also be available to the Head of School/Headteacher/Deputy Headteacher/ICT Technician and kept in a secure, physical (e.g. fire safe) or electronic location software with encrypted storage. The school, in conjunction with the ICT support provider, will use a sufficient Internet filtering system to restrict access to certain materials, adhering to current government guidelines and recommendations. However, the school is aware that children must be educated in how to deal with inappropriate material.

Pupil's responsibilities

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression,

with opportunities for creative activities. E-safety should be referenced in all areas of the curriculum and staff should reinforce e-safety messages whenever ICT is being used.
A planned e-safety programme will be provided as part of both ICT and PSHCE lessons and will be regularly revisited – this will cover the use of ICT both in and outside school and will include:

- The safe and responsible use of the Internet
- The safe and responsible use of mobile devices
- The safe and responsible use of social media
- The management of digital identity

Whenever the Internet is used for research, pupils should be taught to be critically aware of the content they access online and be guided to validate the accuracy of information. It is accepted that pupils may need to research topics (e.g. racism, drugs and discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request a temporary removal of those sites from the filtered list for the period of study. Any request to do so should be auditable, time-limited and with clear reasons given.
We do not recommend that pupils bring mobile devices into school, however, in instances where parents of Year 5 and 6 pupils are allowing children to walk to/ from school alone, we understand that they may wish to supply a mobile phone. In these instances, the child must hand their phone in to the phone box at the start of the day and collect it at the end. Children must not switch their phones back on until they have left the school site.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Responding to incidents of abuse and misuse

At Sketchley Hill Primary School, we understand the importance of acting on reported incidents of abuse and misuse of our ICT systems in school. The incidents may involve illegal or inappropriate activities. Sketchley Hill Primary School actively encourages a safe and secure approach to the management of the incidents.

Pupils are encouraged to report any incidents immediately to a member of staff. Staff will liaise with the Senior Leadership Team and the Designated Safeguarding Lead, ICT support as necessary to investigate the alleged incident and establish evidence of any breach or wrongdoing. Staff will:

- Work with any pupils involved to resolve issues and educate users as necessary.
- Inform parents/carers of the incident and any outcomes.
- Where the alleged incident involves staff misuse, the Headteacher/Deputy Headteacher should be informed.
- Outcomes of investigations will be reported to the Head teacher/Deputy Head teacher and to external services where appropriate (e.g. Social Services, Police Service, the Child Exploitation and Online Protection Service). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- Where the alleged incident involves misuse by the Headteacher, the Chair of Governors should be informed.

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Positive Behaviour Policy.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyberbullying with their classes, and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health, citizenship and economic (PSHCE) education, and other subjects where appropriate.

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Useful websites

www.gov.uk
In the search box at the top of the page type:

- Preventing and tackling bullying
- Searching, screening and confiscation at school
- The Prevent Duty

www.leicestershire.gov.uk
In the search box at the top of the page type:

- E-Safety

www.thinkuknow.co.uk
Thinkuknow is the education programme from CEOP, a UK organisation that protects children both online and offline.
Explore one of the six Thinkuknow websites for advice about staying safe when you are on a phone, tablet or computer.

Acceptable use of the internet in school / data protection

All pupils, parents, staff, volunteers and governance members are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Use of live streaming within school will be monitored and only done in public view with a member of staff present. Privacy and safety settings are in place.

Children will be taught about online safe and unsafe behaviours to make sure that they are aware of what they are posting online. Children will know who to go to for help and how to report things that concern them.

We will monitor the websites visited by pupils, staff, volunteers, governance members and visitors (where relevant) to ensure they comply with the above.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. This will be through the schools own CPD programme.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, ebulletins and staff meetings).

The DSL and Deputy DSL's will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governance members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

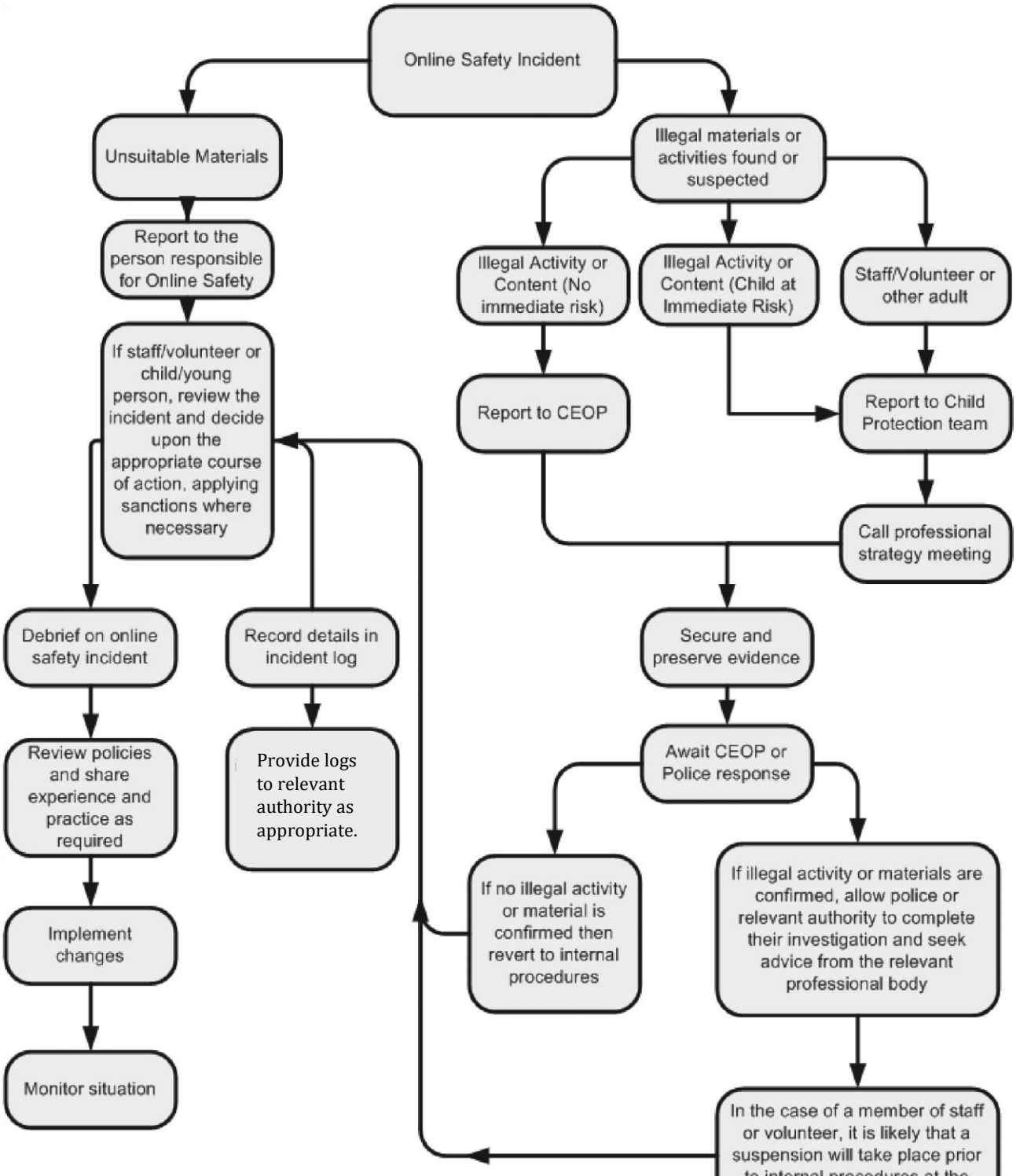
Volunteers will receive appropriate training and updates, if applicable.

Review

This policy will be reviewed every two years by the Computing Lead, DHT and HT and will be shared with all stakeholders where relevant.

Reporting of Online Safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:



CEOP = Child Exploitation and Online Protection Centre found at http://ceop.police.uk /

Acceptable Use Agreement for Staff, Governors and Volunteers

ICT and related technologies such as email, the Internet and mobile devices are an expected part of working life in school. This agreement is designed to ensure that Governors and volunteers are aware of their professional responsibilities when using any form of ICT.

Before becoming school ICT users, you are always asked to sign this policy and adhere to its contents. Any concerns or clarification should be discussed with the Headteacher, who is the E-Safety Co-ordinator.

General:

- I have read the school E-safety Policy.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not install any hardware or software without the permission of the E-Safety lead.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only take images of pupils and/or staff for professional purposes in line with school policy.
- I will not distribute images outside the school network/learning platform without the permission of the Headteacher.
- I will report any incidents of concern regarding children's safety to the E-Safety Co-ordinator, the Designated Safeguarding Lead or Headteacher.

Wi-Fi/Internet use:

- I will only use the school's email/Internet/Intranet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all use of the Internet and other related technologies can be monitored, logged and can be made available, on request, to the Headteacher.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not make copies or download any school based information on my home devices.
- Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or the Chair of Governors.

I agree to follow this code of conduct. I understand that the sanctions for disregarding any of the above will result in removal of access to ICT infrastructure and serious infringements may be referred to the police.

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, carers and other professionals, they are asked to sign this agreement. Members of staff should consult the E-Safety Policy for further clarification of their responsibilities.

- I understand that it is a criminal offence to use any school ICT resource for a purpose not permitted by its owner.
- I understand that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email and social networking; and that ICT use may also include personal ICT devices when used for school business.

- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will log off or lock the computer/device I have been using when leaving it unattended.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised ICT support person.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off site or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to a Designated Safeguarding Lead or a member of the Senior Leadership Team.
- I will ensure that electronic communications with pupils including email and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I will only utilise the school email platform to communicate any school matters.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I agree to follow this code of conduct. I understand that the sanctions for disregarding any of the above will result in removal of access to ICT infrastructure and serious infringements may be referred to the police.

Full Name ……

Signature …… Date ……......

Acceptable Use Statement for pupils

As pupils at Sketchley Hill Primary School, we want you to enjoy using the computers within our school.

It is very important that you:

Always look after the equipment

Be **kind** to one another, **sharing** the equipment nicely and fairly 

Make sure you use **kind language** when talking to others through the computer

Only use websites or play games that your teacher has **allowed** you to use 

Tell your teacher if anything or anyone makes you **feel uncomfortable** or if there is a problem

Do not bring to school any mobile phone or tablet from home (unless agreed otherwise with the school). 

Remember not everything you read on the Internet may be true

Remember that sometimes attachments can contain **viruses or bugs** so only open attachments from people you know. 

I UNDERSTAND THAT THIS IS IMPORTANT, SO I PROMISE TO:

- Only use the Internet and email when an adult is nearby
- Only click on icons and links when I know they are safe
- Only send friendly and polite messages
- Never share my usernames and passwords
- Always tell an adult if I see something I don't like on a screen

LOCKI SAYS KEEP SAFE