Sutton Veny CE Primary School
Online Safety Policy

Development, Monitoring and Review of this Policy

This online safety policy has been developed by the Headteacher, (Adam Lewis) the Online Safety Lead (Ali Dale) and staff, and approved by the Governors of the school. It 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 school will monitor the impact of the policy using logs of reported incidents and through communication with pupils, parents/cares and staff.

This policy applies to all members of the school community who have access to and are users of school/academy digital technology systems, both in and out of the school.

Online Safety

It is essential that children are safe from potentially harmful and inappropriate online material. An effective whole school approach on online safety empowers us to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in and escalate any concerns where appropriate.

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.

Whilst considering our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the school does everything possible to limit children's exposure to the above risks from the school's IT system.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This is carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor and this role includes:

- regular meetings with the Online Safety Leader
- attendance at Online Safety Group meetings

- regular monitoring of online safety incident logs
- reporting to relevant Governors meetings
- attending online safety training and information sessions

Headteacher and Senior Leaders:

- are aware of the procedures to be followed in the event of an online safety incident or allegation. See flow chart 'Responding to Incidents of Misuse' (Appendix 1).
- creates a log of incidents to inform future online safety developments
- ensures that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles
- in accordance with the Education and Inspections Act 2006, deals with incidents of inappropriate online safety behaviour that take place out of school, and inform parents/carers

Online Safety Lead:

- establishes and reviews the school online safety policies and documents, and presents any updates for discussion with staff
- 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 school technician (Austen Chaloner of MARC Computers) to ensure that the technical infrastructure is secure, the school meets required online safety technical requirements, including filtering and virus protection, and that the appropriate access is provided for users.
- has access to the administrator password for the server
- ensures that the software licence logs are accurate and up-to-date
- attends relevant meetings with the Online Safety Governor to discuss current issues
- meets with Digital Leaders to share the pupils' views on online safety (Appendix 5c)
- reports regularly to the Senior Leadership Team
- monitors improvement actions identified through use of the 360° safe self-review tool
- plans a differentiated online safety curriculum, appropriate to each age group
- ensures that key online safety messages are reinforced through relevant assemblies
- receives regular updates through attendance at external training events and by reviewing guidance documents

Designated Safeguarding Lead (DSL)

The DSL is trained in online safety issues and 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

Teaching and Support Staff:

- have an up to date awareness of online safety matters and of the current school online safety policy and practices and understand their responsibilities
- receive online safety training as part of induction and subsequently every three years
- have read, understood and signed the Staff Acceptable Use Policy (Appendix 2)
- report any suspected misuse or problem, including inappropriate emails, to the Headteacher or Online Safety Lead
- carry out all digital communications with pupils and parents/carers on a professional level and only using official school systems
- embed online safety issues in all aspects of the curriculum
- ensure that all areas of the online safety are covered for that year group
- ensure pupils understand and follow the online safety procedures and acceptable use policies
- ensure pupils have a good understanding of research skills including how to avoid plagiarism and uphold copyright regulations
- always monitor the use of digital technologies and the internet in school
- guide pupils to websites that have been checked as suitable for their use and know how to deal with any unsuitable material that is found in internet searches
- teach children to be critically aware of the content they access on-line with regard to the accuracy of information (Upper KS2)
- support children to be aware of radicalisation and sexting (Year 6)
- act as good role models in their use of digital technologies, the internet and mobile devices
- use secure passwords to access the relevant areas of the server (Appendix 8)
- can temporarily unblock filtered sites for educational purposes only
- will not use pupil's full names anywhere on the website
- must see the Online Safety Lead regarding installing programmes onto school devices
- must not take personal data off the school site unless it is encrypted or password protected. See Data Protection Policy (Appendix 3)
- take digital/video images, using school devices, to support educational aims and follow school policies concerning the sharing, distribution and publication of those images
- staff must not use personal devices to take videos or images. Mobile phones must be silenced in the classroom.
- are allocated with a safe, monitored, school email address and this must be used for any digital communication with parents/carers, pupils and outside agencies, using professional tone and content as stated in the Staff Acceptable Use Policy
- must not post any content on social media sites that will bring the school into disrepute or breach confidentiality, as explained in the Personal Use of Social Media Policy (Appendix 4)

Pupils

The education of pupils in online safety and digital literacy is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. The pupils

- are responsible for using the school digital technology systems in accordance with the pupil's Acceptable Use Agreement that they sign annually in their Link Books (Appendix 5a and b)
- are taught to tell an adult if anything is worrying them online, including texts and emails, and are taught how report abuse or misuse at KS2
- 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
- access the server through class (FS2 – Year 4) or individual (Year 5 – Year 6) passwords
- are not allowed to bring their own mobile devices to school, including phones
- must not take images of others without their permission
- use a whole class email address when sending emails, writing their messages in a polite and friendly manner

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school takes every opportunity to help parents understand these issues through newsletters, the website and national online safety campaigns. Parents and carers are 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 Learning Platform
- provide written consent before photographs of pupils are published on the school website or in the local press
- sign the pupil's Acceptable Use Agreement that they sign annually in their Link Books (Appendix 5a and b)
- are welcome to take videos and digital images of their children at school events for their own personal use. They are requested not to share these on social networking sites
- any devices that are borrowed from school for home use e.g for home learning during a pandemic (Appendix 6a and b)

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign an Acceptable Use Agreement (Appendix 7a and b) before being provided with access to school systems. Guests such as trainee teachers, supply teachers and visitors will be provided with temporary passwords to access the school systems.

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 to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

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.

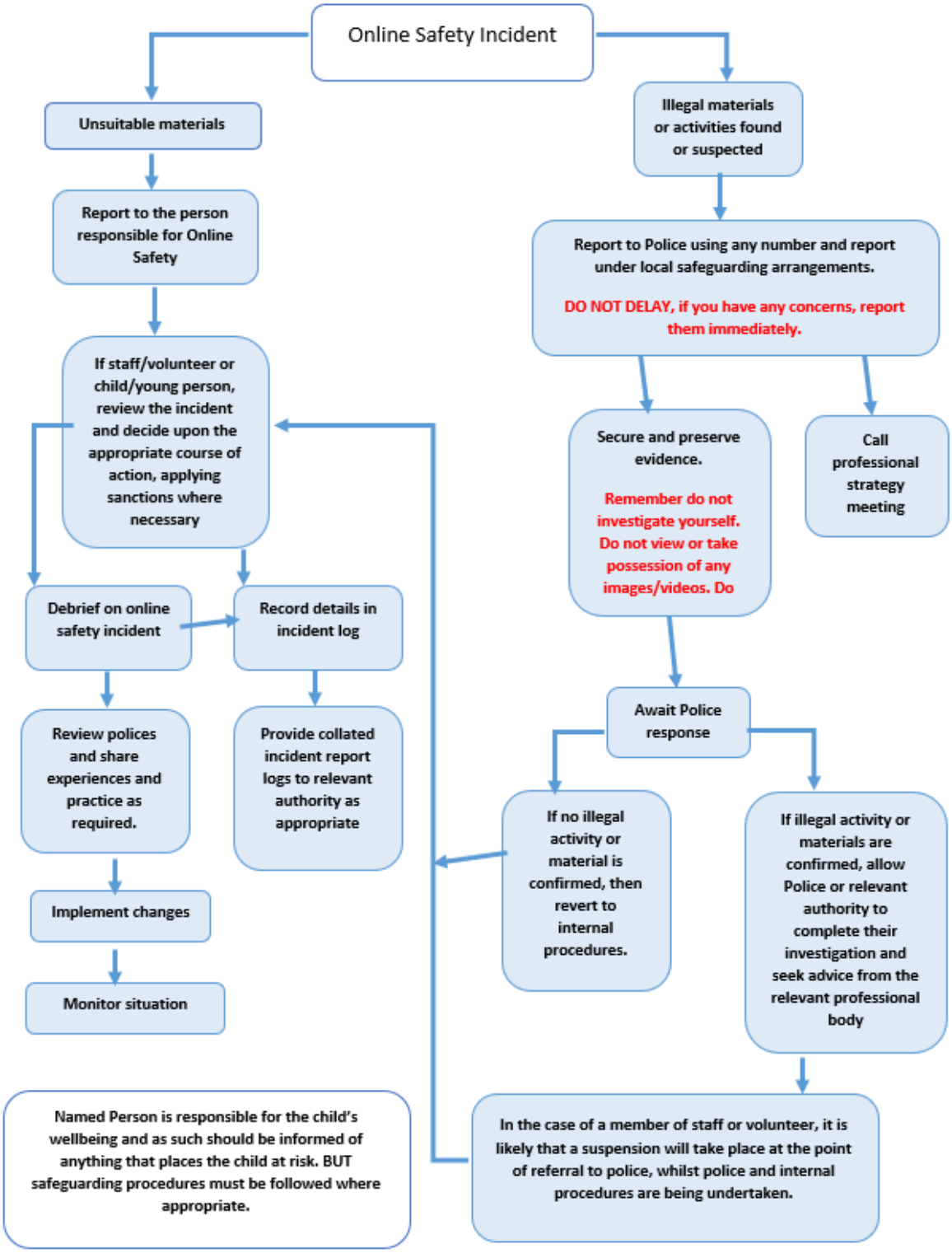
In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff 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/Academy Group 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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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 form should be retained by the group for evidence and reference purposes.

Appendix 1

Responding to Incidents of Misuse



Appendix 2

Online Safety: Staff Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital 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 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 pupils' 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 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, virtual learning environments (VLE) etc.) out of school, and to the transfer of personal data (digital or paper based) 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, nor 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 Online Safety Lead or Headteacher.

I will be professional in my communications and actions when using school 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/VLE) 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 students/pupils and 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

- I will not use personal email addresses on the school ICT systems.
- 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, terrorist or extremist 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 try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Secure Data Handling Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when that I am required to disclose such information to an appropriate authority.

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

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) within these guidelines.

Name: .....

Signed: .....

Date: .....

Appendix 3:

Data Protection Policy

Introduction:

Staff have access to a wide range of sensitive information, both personal data of staff and pupils, and financial data. Both types of information are managed in a secure way at all times. Personal data is defined by the Data Protection Act as **"Data relating to a living individual who can be identified from the data".**

Data is:

- processed fairly and lawfully
- collected for a specified purpose and not used for anything incompatible with that purpose
- adequate, relevant and not excessive
- accurate and up-to-date
- not kept longer than necessary
- processed in accordance with the rights of the data subject
- kept securely
- not transferred outside the EEA (European Economic Area) unless the country offers adequate protection.

In accordance with The Data Protection Act the following types of personal information receive higher level of protection, including information relating to:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life (orientation)
- the commission or alleged commission by them of any offence, or any proceedings for such or the sentence of any court in such proceedings.

Information needs to treated securely if loss or disclosure

- places anyone at risk
- causes embarrassment to an individual or the school
- has legal or financial implications (see Appendix A)

Procedures and Practice:

- The amount of data held is reduced to a minimum.
- Data is assessed to consider whether it still needs to be kept or not.
- Personal data is securely stored and sent by secure means.

Auditing:

- The school is aware of **all** the sensitive data it holds, be it electronic or paper.
- A register of data is kept and updated as necessary
- How long these documents need to be kept is assessed using the Records Management Toolkit.
- Audits will take place in line with the timetable. (Appendix C).

- The audit will be completed by a member of staff responsible for data protection.

Risk Assessment:

The school will regularly carry out a risk assessment to establish what security measures are already in place to ascertain;

- the sensitivity is the data
- the likelihood of it falling into the wrong hands
- the impact of this
- further actions

Securing and Handling Data Held by the School:

- Any data that is determined to be personal or commercially sensitive in nature will be encrypted. This includes fixed computers, laptops and memory sticks.
- Staff should **not** remove or copy sensitive data unless the media is encrypted, transported securely and stored in a secure location.
- Data should be sent through secure emails with password protection; the password must be sent by other means and not included in the same email.
- Data (pupil records, SEN data, contact details, assessment information) will be backed up, encrypted and stored in a secure place – e.g. safe / fire safe / remote backup.
- All staff computers will be used in accordance with the Teacher Laptop Policy (Appendix D)
- When laptops are passed on or re-issued, data is securely wiped from any hard drive before the next person uses it. This is done our technician using a recognised tool.
- The school's wireless network (WiFi) is be secure at all times.
- Remote access off the school site to any personal data is achieved using an encrypted connection and protected by a username/ID and password. This information is not stored on a personal (home) computer.
- The school will keep necessary pupil and staff information in accordance with the Records Management Society's guidance (see references at the end of this document).
- All staff are trained to understand the need to handle data securely.

References:

The Data Protection Act 1998:
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
Information Commissioner's Office
www.ico.gov.uk
Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008
https://www.gov.uk/government/publications/information-sharing-for-practitioners-and-managers

Records Management Society – Tool Kit for Schools:
http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school

This policy should be read and understood in conjunction with the following policies and guidance:

- The Data Protection Act 1998
- Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008
- Records Management Society – Tool Kit for Schools

Appendix 3A: Assessing risk of sharing information

In case of security breach:

- Will it affect or identify any member of the school or community?
- Will someone lose / be out of pocket by / more than £100?
- Will it cause any kind of criminal case to fail?
- Is there a risk of discomfort / slur upon professional character of someone?
- Is anyone's personal safety at risk?
- Will it embarrass anyone?

If **yes** to any of the questions, the document with include some sensitive information and therefore requires a level of protection.

In case of security breach

- Will it affect many members of the school or local community and need extra resources locally to manage it?
- Will an individual lose / be out of pocket by £1,000 to £10,000?
- Will a serious criminal case or prosecution fail?
- Is someone's personal safety at a moderate risk?
- Will someone lose his or her professional reputation?
- Will a company or organisation £100,000 to £1,000,000?

If **yes** to any of the questions additional security should be considered.

Appendix 3B: Register of sensitive data held by the school

Type of data	**Held on**	**Period to be retained**	**Type of protection**	**Who can access the data**
Pupil SEN data	SENCO laptop and School Server	While pupils are on role at Sutton Veny School – passed on to receiving school	Data is encrypted on laptop	SENCO and Headteacher
Staff Personal Data	School Server	While employed at the school	Data in encrypted	Office Staff and Headteacher
Pupil Personal Data	School Server	While pupils are on role	Data in encrypted	Office Staff and Headteacher

Appendix C: Timetable for Information Security Management

Activity	**Frequency**	**Lead**
Audit of data held	Annually	Head and admin officer
Encrypting sensitive data	On-going	All staff
Reviewing data backup procedures	Annual	Admin officer
Identifying staff responsible for data security and keep log of names and roles.	Annual	Head
Wiping of laptop data when re-issued	Annual and then when necessary.	ICT Technician
Wiping of laptop data when discarded	As necessary	ICT Technician

Appendix 4:

Online Safety: Personal Use of Social Media Policy

Introduction

This policy is one of a set of policies governing the conduct of employees of Sutton Veny CE Primary School. Social media is a type of interactive online communication that allows parties to communicate instantly with each other or to share information in a public forum. There are various online technology tools that enable people engage in social media.

This policy provides guidance to school employees who use social media sites in their personal time (either at home or during an authorised break at work), with the aim of protecting both staff and the school from disrepute.

The governing body of Sutton Veny CE Primary School has agreed to adopt this policy. The policy will be applied to all permanent, temporary and casual employees employed at the school.

This policy applies at all times when school employees are making use of social media sites in a personal capacity. It applies whether the employee is at home or at work and whether they are using school equipment or their own device.

This policy does not cover the use of social media sites by employees within their role on behalf of the school. Where employees use social media sites as part of their work the school will make them aware of the school's expectations and standards in the use of social media via that separate policy.

Social media etiquette

Social media allows people great freedom in how they communicate and express themselves. To help ensure everyone is able to equally benefit from social media sites, employees at Sutton Veny CE Primary School must abide by the following principles:

- tell the truth;
- write deliberately and with accuracy;
- acknowledge and correct mistakes promptly;
- preserve the original post, using notations to show where changes have been made, so as to maintain the integrity of any material published
- never delete someone else's post, although a poster could delete their own post.
- give due consideration when posting comments and have regard to the advice within this policy;
- strive for high quality with every post – including basic spellchecking;
- stay on topic;
- disagree with other opinions respectfully;
- link to online references and original source materials directly;
- disclose conflicts of interest;
- keep private issues and topics separate from work issues and topics.

Many employees make use of social media in a personal capacity and this policy is not intended to limit their use or enjoyment of social media. However, employees should remember that, even when not acting on the school's behalf, they can be held accountable for content which they post on social media sites which could be potentially damaging to the school. Damaging content includes any communication made in a personal capacity through social media which:

Brings the school into disrepute	e.g. criticising the school, pupils or colleagues/governors in an inappropriate manner, posting images that are inappropriate or links to inappropriate content.
Breaches confidentiality	e.g. revealing information owned by the school; giving away confidential information about an individual (such as a colleague or pupil) or discussing the school's internal workings (such as school budget spending that have not been communicated to the public)
Is discriminatory against, or bullying or harassment of, any group or individual	e.g. making offensive or derogatory comments relating to sex, gender reassignment, race (including ethnicity), disability, sexual orientation, religion or belief or age; using social media to bully another individual; or posting images that are discriminatory or offensive, or links to such content.
Breaches copyright	e.g. by using someone else's images or written content without permission.

Employees:

- must consider who can read what is posted, they must be aware that some sites are open to all and other sites allow the employee to control who can see what has been posted
- must carefully consider, before posting content on social media sites, whether this will bring the school into disrepute, breach confidentiality or copyright or be considered offensive, defamatory, discriminatory, bullying or is potential harassment
- need to ensure that they have reviewed privacy settings so that only those who they wish to read the content are able to do so
- should not include their workplace and/or job title on their profile, being aware that this may make it easier for pupils, parents and members of the public to contact them in their personal time
- should make it clear that they are not representing the school when commenting in a personal capacity on any issues relating to the school, and that the views expressed are personal and do not necessarily reflect the views of the school
- may make occasional and reasonable personal use of the internet (for example during their lunch break), as long as this does not interfere with the performance of their duties or the work of other colleagues
- must only access social media sites for personal use on their own equipment (e.g. mobile phone, smartphone etc.) during official breaks

The school:

- will monitor social media websites in the same way as it monitors other media channels (e.g. local press etc.) for relevant content about the school
- will not routinely monitor the webpages that an employee can access from their school laptop, however full logs are retained and can be accessed as part of a genuine investigation

- does not monitor employee's personal social media pages without reason. However, as with any allegation of misconduct, the school will investigate where breaches of this policy are brought to its attention by any means

Investigation which involves social media content will take into consideration the intent of the content, what damage has been done, the implications, the impact and the individual's right to freedom of expression (provided it is not discriminatory, damaging, malicious or libellous).

Inappropriate content posted on social media sites either during, or outside of work time, may lead to either informal or formal disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues, discriminatory behaviour or social media activity causing serious damage to the school, may constitute gross misconduct and lead to summary dismissal. Social media content which proves that employees have breached other school policies may be used in disciplinary investigations relating to these matters.

This policy has been Equality Impact Assessed to identify opportunities to promote equality and mitigate any negative or adverse impacts on particular groups.

Legislation and guidance:

Human Rights Act 1998
Data Protection Act 1988
Equalities Act 2011
ACAS Factsheets "Social Networking"
Guidance for safer working practice for adults who work with children and young people in education settings

Further information:

There are a number of related policies and procedures that employees should be aware of including:
Code of Conduct
Dignity at work
Disciplinary policy and procedure
Grievance policy and procedure
Whistleblowing policy

In addition, employee's job descriptions may contain requirements relating to their conduct. There are also professional codes of conduct e.g. teacher's standards, that relate to the work an employee does and how it is done.

Appendix 5a

Sutton Veny Responsible Use Agreement for FS2/KS1 Children

Parent/Carer's Signature: ..... Date: .....

Child's Signature: .....

Appendix 5b:

Responsible Use Agreement for KS2 Children

☺ I will **always** look after the computing equipment and not damage it in any way.

☺ I will ask permission from a member of staff before using the Internet.

☺ I will only visit websites to help me with schoolwork or homework or that my teacher has said I can go on.

☺ I will only send messages to people that my teacher has agreed to.

☺ The messages I send and the work I do will be polite and responsible, and not contain anything that might upset someone else.

☺ I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.

☺ I will keep my usernames and passwords safe by not telling anyone else.

☺ I will not change any settings on the computers or iPads at school.

☺ I will tell an adult if there is something wrong with the computer or iPad and not try to fix it myself.

☺ I will only change or delete my own files.

☺ I will only look at other people's files or messages with their permission.

☺ I will always close down the computers and iPads properly after use.

I UNDERSTAND THAT I MUST FOLLOW THESE RULES.

Pupil's signature: Class:

Parent/Carer's signature: Date:

Appendix 5c:

Responsible Use Agreement for Digital Leaders

☺ I will be a polite and helpful Digital Leader!

☺ I will make sure that I get my own work done as well as help my classmates.

☺ I will teach my classmates how to do something rather than just do it for them.

☺ I will keep all passwords and usernames a secret.

☺ When I am using the teacher's laptop I will never look at or click on any of the teacher's work.

☺ I will make sure the iPads and laptops are put away carefully and safely.

☺ I will check that the laptops are plugged in, charging and do not have any thing placed on top of them.

☺ I will let my teacher know if there are any problems with the iPads or laptops.

I WILL TRY MY BEST TO FOLLOW THESE RULES.

Pupil's signature: Class:

Appendix 6a:

Acceptable Use Policy for Devices at Home

1. The device remains the property of Sutton Veny Primary School.

2. The device is allocated to a named adult/child and is their responsibility. Please do not lend it to other people.

3. Please only use the device for the intended purpose.

4. The device must not be used for general internet use. Please do not use it for personal shopping or social networking.

5. After use the device is returned to Sutton Veny School for use by other families.

6. Whenever possible, the device must not be left in an unattended car. If there is a need to do so it should be locked in the boot.

7. If any removable media is used then it must be checked to ensure it is free from any viruses.

8. Please do not attempt to alter the computer settings. The devices should not be synced with any devices in the household.

9. Please do not download new apps but let us know if you would like certain apps available.

10. If any fault occurs with the device, it should be referred immediately to the Online Safety Lead (Mrs Ali Dale).

11. The device would be covered by normal household insurance.

12. I understand that the school may, in line with policy, monitor and check my e-mails.

13. Activity that threatens the integrity of the school is forbidden.

14. Please take great care of the device. We would like to be able to offer it to other families in good working condition.

Name: .....

Signature: ..... **Date:** .....

Appendix 6b:

Pupil's Responsible Use Agreement for Device Home Use

☺ I will **always** look after the iPad and not damage it in any way.

☺ I will ask permission from an adult before using the Internet.

☺ I will only visit websites that an adult has said I can go on.

☺ I will only send messages to people that my teacher has agreed to.

☺ I will ask my teacher to download new apps rather than doing it myself.

☺ The messages I send and the work I do will be polite and responsible, and not contain anything that might upset someone else.

☺ I will always use what I have learned about e-safety to keep myself safe and will tell an adult if something makes me worried or unhappy.

☺ I will keep my usernames and passwords safe by not telling anyone else.

☺ I will not change any settings on the iPads.

☺ I will tell an adult if there is something wrong with the iPad and not try to fix it myself.

☺ I will only change or delete my own files.

☺ I will only use the iPad to talk to and share things with my parent that is away.

I UNDERSTAND THAT I MUST FOLLOW THESE RULES.

Pupil's signature: Class:

Parent/Carer's signature: Date:

Appendix 7a:

Online Safety: Acceptable Use Policy Agreement for Governors and Friends of School

1. I will use the email account issued to me in an appropriate way. I will not:
   - access offensive emails or download offensive material
   - make personal use of the e-mail account
   - copy information from the Internet that is copyright or without the owner's permission
   - send e-mails that are offensive or otherwise inappropriate
   - disregard my responsibilities for security and confidentiality
   - access the files of others or attempt to alter the email account settings.
2. I will only access the account with my own name and registered password, which I will keep secret.
3. I will inform the Head Teacher as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working. ·
5. I understand that the school may, in line with policy, monitor and check my e-mails.
6. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
7. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Head Teacher.
8. All joke e-mails and attachments are potentially damaging and undesirable and therefore must not be used.
9. I will report immediately to the Head Teacher any unpleasant material or messages sent to me.
10. Activity that threatens the integrity of the school is forbidden.
11. I understand that if I do not adhere to these rules my email account will be suspended immediately and that other disciplinary consequences may follow.

Name: .....

Signature: ..... **Date:** .....

Appendix 7b:

Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- 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 will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

- I understand that if I fail to comply with this acceptable use agreement, the school/academy has the right to remove my access to school systems/devices

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.

Name: ..... Signed: ..... Date: .....

Appendix 8

Online Safety: Password Security Policy

Introduction

The school is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled

Responsibilities

The management of the password security policy will be the responsibility of the Online Safety Lead. All adults will have responsibility for the security of their username and password. Adults must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Training and Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Policy Agreement
- through regular online safety training

Pupils will be made aware of the school's password policy where appropriate:

- in Computing, PSHE or e-safety lessons
- through the use of posters placed in classrooms
- through the Responsible Use Agreement
- through online safety focus days

Infrastructure

All users will have clearly defined access rights to school ICT systems. The server has separate areas of access for

- pupils
- teachers
- admin and Headteacher

Staff laptops are password protected. Passwords are not displayed on screen, and shall be securely hashed. Confidential information is stored on encrypted USB pens.

The administrator passwords for the school computer system, used by the technician, are available to the Headteacher and Online Safety Lead and kept in a secure place. The school does not allow one user to have sole administrator access.

Local Authority Auditors have the right of access to passwords for audit investigation purposes. In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.