YATTON SCHOOLS

E-SAFETY POLICY

Document Information			
Reviewed by:	PQA	**Responsibility:**	PQA
Last Review:	October 2022	**Next Review:**	October 2023
Review Cycle:	Annually	**Ratified by FGB**	Not required
Signature (FGB)	Not required	**Signature (Head)**	Not required

To be read in conjunction with:

- Acceptable Use Policy Agreement for Staff (Appendix A);
- Acceptable Use Policy Agreement for Pupils (Appendices B; C; D)
- Acceptable Use Policy for Volunteers, Visitors and Community Users (Appendix E)
- Safeguarding Policy
- Anti-Bullying Policy
- Behaviour & Discipline Policies
- Social Media/Networking Policy
- Photographic Images in School Policy
- Data Handling Policy

RATIONALE

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. We recognise that the internet and other digital and information technologies are powerful tools, which can stimulate discussion, promote creativity and promote effective learning. However, the use of these technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to /loss of /sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video films
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing

wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

MONITORING & REVIEW OF POLICY

The implementation of this policy will be monitored and reviewed by the IT Lead, the E-Safety Governor and the School Leadership Team at least annually or more frequently in light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. The E-Safety Governor will report to the Governor's PQA Committee on the implementation of this policy at least annually. (KCSIE 2022 –p36-37)

The policy will be monitored through:

- Logs of reported incidents;
- RM Safety Net – creates reports and allows the school to block sites
- Cyber Alarm – (Police checks through a virtual server linked to the school server)
- Surveys/questionnaires of learners, parents and staff.

SCOPE OF POLICY

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

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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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 e-safety behaviour that take place out of school.

ROLES AND RESPONSIBILITIES

Role	Responsibility
Governors	• Approval of the E-Safety policy and for reviewing its effectiveness. • Appoint a member of the Governing Body as E-Safety Governor. The role of the E-Safety Governor will include: • regular meetings with the IT Lead and SLT • regular monitoring of e-safety incident logs • regular monitoring of filtering/change control logs • reporting to relevant Governors committee
Headteacher and Senior Leadership Team	• The Headteacher is responsible 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 IT Lead or School IT Technician. • The Headteacher and SLT are responsible for ensuring that the IT Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant. • The Headteacher and SLT 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 support to those colleagues who take on important monitoring roles. • The Headteacher and other members of the SLT will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. • Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. • Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. • Liaises with school ICT technical staff. • Meets with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs. •
Computing Lead	• Leads meetings with the SLT and E-Safety Governor • Provides training and advice for staff. • Liaises with the Local Authority and/or Trust • Liaises with school ICT technical staff. • Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
ICT Technician	The ICT Technician is responsible for ensuring: • That the school's ICT infrastructure is secure and is not open to misuse or malicious attack. • That the school meets the e-safety technical requirements outlined in the Soltech /SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority / Trust E-Safety Policy and guidance. • That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed. • 2IT /RM Safety Net /SWGfL is informed of issues relating to the filtering applied by the Grid. • That he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • That the use of the network is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher / SLT for investigation, action, sanction. • That monitoring software/systems are implemented and updated as agreed in school policies.
Teaching and Support Staff	Responsible for ensuring that: • They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices. • They have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP) and Trust Code of Conduct. • They report any suspected misuse or problem to the IT Lead of SLT for investigation/action/sanction. • Digital communications with pupils should be on a professional level and only carried out using official school

	systems. • E-safety issues are embedded in all aspects of the curriculum and other school activities. • The school's e-safety and acceptable use policy is shared and understood by pupils. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • They monitor IT activity in lessons and extra-curricular activities. • They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. • In lessons where internet use is pre-planned, 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. • Appropriate security settings are in place for use of social networking sites, so to protect professional identity and the safety of pupils. • School business or dialogue regarding pupils and colleagues is not shared digitally via social networking sites.
Pupils	Are responsible for using the school ICT systems in accordance with the appropriate Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. • Have an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying. • Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school. • Follow the rules of safe use of Microsoft Teams (see Appendix F)
Parents/Carers	Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and website information about national/local e-safety campaigns/literature. Parents and carers will be responsible for: • Endorsing (by signature) the Pupil Acceptable Use Policy
Volunteers/Visitors and Community Users	Volunteers as well as those community users who access school ICT systems as part of the schools' Extended Schools provision will be expected to sign an AUP before being provided with access to

	school systems.

ICT within the Curriculum

A planned e-safety programme, highlighting key e-safety messages, will be provided as part of the Computing Curriculum and PSHE lessons, and will be regularly revisited; this will cover both the use of ICT and new technologies in school and outside school. Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices, both within and outside school.

Pupils will 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. They will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Rules for the use of ICT systems and the internet will be posted in classrooms and in the ICT suites. Members of staff will act as good role models in their use of ICT, the internet and mobile devices.

E-Safety will be a focus in all areas of the curriculum and staff will reinforce e-safety messages in the use of ICT across the curriculum. In lessons where internet use is planned, it is best practice that pupils are guided to sites pre-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, e.g. using search engines, staff will be vigilant in monitoring the content of the websites visited.

It is accepted that, from time to time, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the E-Safety/ICT Technician can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be recorded to provide an audit trail with clear reasons for the need.

Education & Training – Staff

It is essential that staff, according to their role, receive e-safety training and understand their responsibilities as outlined in this policy. Training will be offered as follows:

- Formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly and a log kept of all training undertaken. It is expected that some members of staff will identify e-safety as a training need within their performance management process.
- New staff will receive e-safety training as part of their induction programme, ensuring that they fully understand and sign the school's E-Safety Policy and Acceptable Use Policies;
- The IT subject leader will receive regular updates through attendance at network/SWGfL/Trust /other information / training sessions and by reviewing guidance documents released by the RM Safety Net/ SWGfL, the Trust, Local Authority and others.
- The IT subject leader will provide advice/guidance/training to individuals as required.
- E-Safety training and updates will be delivered to school staff as part of INSET training each year. The E-Safety Policy and AUPs will be discussed and signed as part of this training. Further training and updates will be provided at staff/team meetings as appropriate.

Technical Issues

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Appropriate security measures will be in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school's systems and data.

School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the 2IT/SWGfL Security Policy and Acceptable Usage Policy and any relevant Trust (Local Authority E-Safety Policy and guidance). There will be regular reviews and audits of the safety and security of school ICT systems. Servers, wireless systems and cabling must be securely located and physical access restricted.

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed, at least annually, by the E-Safety Committee. All users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. The administrator passwords for the school ICT system, used by the ICT Technician, must also be available to the Headteacher, or other nominated senior leader, and kept in a secure place (school safe). Users will be responsible for the security of their username and password and must not allow other users to access the system using their log on details, and must immediately report any suspicion or evidence that there is a breach of security.

The school maintains and supports the managed filtering service provided by RM Safety Net / SWGfL/ Cyber Alarm. In the event of the ICT Technician needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher. Any filtering issues must be reported immediately to 2IT/ RM Safety Net/ SWGfL. Requests from staff for sites to be removed from the filtered list will be considered by the ICT Technician and ICT Coordinator. If the request is agreed, this action will be recorded and logs of such actions will be reviewed regularly by the E-Safety Committee. All users have a responsibility to report immediately to the ICT Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

ICT technical staff will regularly monitor and record the activity of users on the school's ICT systems and users will be made aware of this in the Acceptable Use Policy.

PASSWORDS

In the interests of everyone's professional and personal safety, the following protocol will be followed by all users (staff and pupils):

- never reveal your password to anyone;
- never use the "remember password" function;
- do not use the same password for systems inside and outside of work;
- do not use any part of your username within the password;
- never write your passwords down or store them where they are open to theft;
- never store your passwords in a computer system without encryption;
- use a "strong" password (use of symbols and characters);
- change your password at least every two terms;

MOBILE PHONES (NB: The term mobile phone includes devices such as Blackberries, I-phones etc)

Pupils

The school recognises that some parents will wish their child to carry a mobile phone so that they may communicate with them before and after the school day. Mobile phones must only be brought to school by with permission from a parent/carer. The following protocol will be followed:

- mobile phones will be switched off during the school day and will not be switched on until the pupil has left the school premises at the end of the day.
- pupils will place their mobile phone in the class teacher's drawer at the beginning of the morning session where it will remain until the end of the afternoon session; mobile phones will not be stored in personal lockers of school bags.
- mobile phones may be collected from the class teacher at the end of the day and will not be removed during the school day unless the class teacher has given specific permission otherwise;

- pupils will not use their mobile phone to make calls, send text messages or take photographs; under no circumstances will pupils be allowed to take photographs of other pupils, members of staff or visitors to the school on their phones.
- pupils will not take mobile phones on school trips or to offsite activities such as sports events. If the pupil is not returning to school after the event, the phone will be left in the care of the teacher in charge until they are collected/go home;
- messages sent from pupils' mobile phones should contain appropriate language and content.
- The use of mobile phones will comply with the Pupils Acceptable Use policy (signed annually by pupils and parents).

Any breach of these rules may result in Sanctions being applied in accordance with the schools' Behaviour Policies.

Staff
It is accepted that the majority of members of staff will have their mobile phone / or iwatch with them at work. (Acceptable use of iwatch to align with expectations of mobile phones for staff.)
To comply with the E-Safety Policy the following protocol will be followed:

- members of staff will act as role models in their use of mobile phones;
- personal mobile phones remain the responsibility of the member of staff at all times;
- mobile phones will be switched off or on silent mode during the school day;
- mobile phones or iwatches will not be used whilst involved in the teaching or supervision of children;
- use of the phone will be limited until break time/non-contact time during the school day and only used in the staffroom, outside the school building and administration offices;
- personal mobile phones must not be used to take or store photographic images of pupils;
- personal mobile phones must not be used to store personal information relating to pupils or parents/carers;
- personal mobile phones must not be used as a means of communication with pupils or parents/carers, unless not to do so places the child at risk of harm;
- the use of personal mobile phones to access inappropriate material/websites whilst onsite /during contractual hours is strictly prohibited.

USE OF DIGITAL IMAGES – PHOTOGRAPHIC / VIDEO (see Photographic Images Policy)
The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate 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.
- Staff 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 must 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 that include pupils published on the website or elsewhere will be selected carefully, will comply with the Schools' Policy on Photographic Images, and will only be published if parental permission has been given.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- 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 school systems. Personal email addresses, text messaging or public chat/ social networking programmes must ***not*** be used for these communications except for the official school twitter accounts set up as a broadcast medium.
- All children will be provided with an individual school email addresses for Microsoft 365 and the use of Teams for educational use/home learning.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material. Guidelines are provided to parents and children before use of Teams. (Appendix F)
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and obviously banned from school and all other ICT systems. Other activities e.g. cyber-bullying is banned and could lead to criminal prosecution. In addition, the Federation believes that the activities outlined below are inappropriate in a school context and users, should not engage in these activities in school or outside school when using school equipment or systems.

- Using school systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Soltech/ SWGfL and / or the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Non-educational online gaming
- Online gambling

- File sharing
- Use of social networking sites except official school twitter accounts.

Social Media Networking

All staff should follow the following guidance / procedures:

- Staff must not access social networking sites for personal use via school information systems or using school equipment;
- Staff must not send any personal messages to pupils – personal communication could be considered inappropriate and unprofessional and makes colleagues at the school vulnerable to allegations;
- Staff are advised not to be friends with recent pupils (the potential for colleagues at the school to be compromised in terms of content and open to accusations makes the risk not worth taking) and staff are also advised not to be friends with pupils at other schools as this is likely to make them vulnerable to allegations and may be open to investigation by the Local Authority or police. Where a colleague is considering not following this advice, they are required to discuss the matter, and the implications with the Headteacher or designated children's safeguarding teacher/officer.
- Any student-initiated communication, on-line friendships/friend requests must be declined and reported to the Headteacher or designated children's safeguarding teacher/officer (If a colleague receives messages on his/her social networking profile that they think could be from a pupil they must report it to their line manager/Headteacher and discuss whether it is appropriate for the colleague to contact the internet service or social networking provider so that the provider can investigate and take the appropriate action);
- staff should not share any personal information with any pupil (including personal contact details, personal website addresses/social networking site details);
- staff should not place/post any material (or links to any material) of a compromising nature (that is, any material a reasonable person might find obscene or offensive (such as sexually explicit or unlawfully discriminatory material) including inappropriate photographs or indecent remarks or material relating to illegal activity) on any social network space;
- staff must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act or disclose any information about the school/ Trust /Local Authority that is not yet in the public arena;
- staff should not post photographs of pupils under any circumstances and should not post photographs of colleagues or parents without their express permission;
- staff should not make abusive/defamatory/undermining/derogatory remarks about the school/colleagues/pupils/parents/governors / Trust or the Local Authority or post anything that misrepresents or could potentially bring the school/Trust/ Local Authority into disrepute;
- staff should not disclose confidential information relating to their employment at the school;
- staff must not link their own sites to the school website or use the school's or the Local Authority's logo or any other identifiers on their personal web pages;
- If any member of staff receives media, contact regarding the content of their site or is offered payment for site content which relates to the school they must consult their Headteacher/line manager;
- No member of staff should use any internet/on-line resources to seek information on any pupil, parent or other colleague at the school other than for the purposes of legitimate monitoring of the usage of Social Networking sites by designated managers.

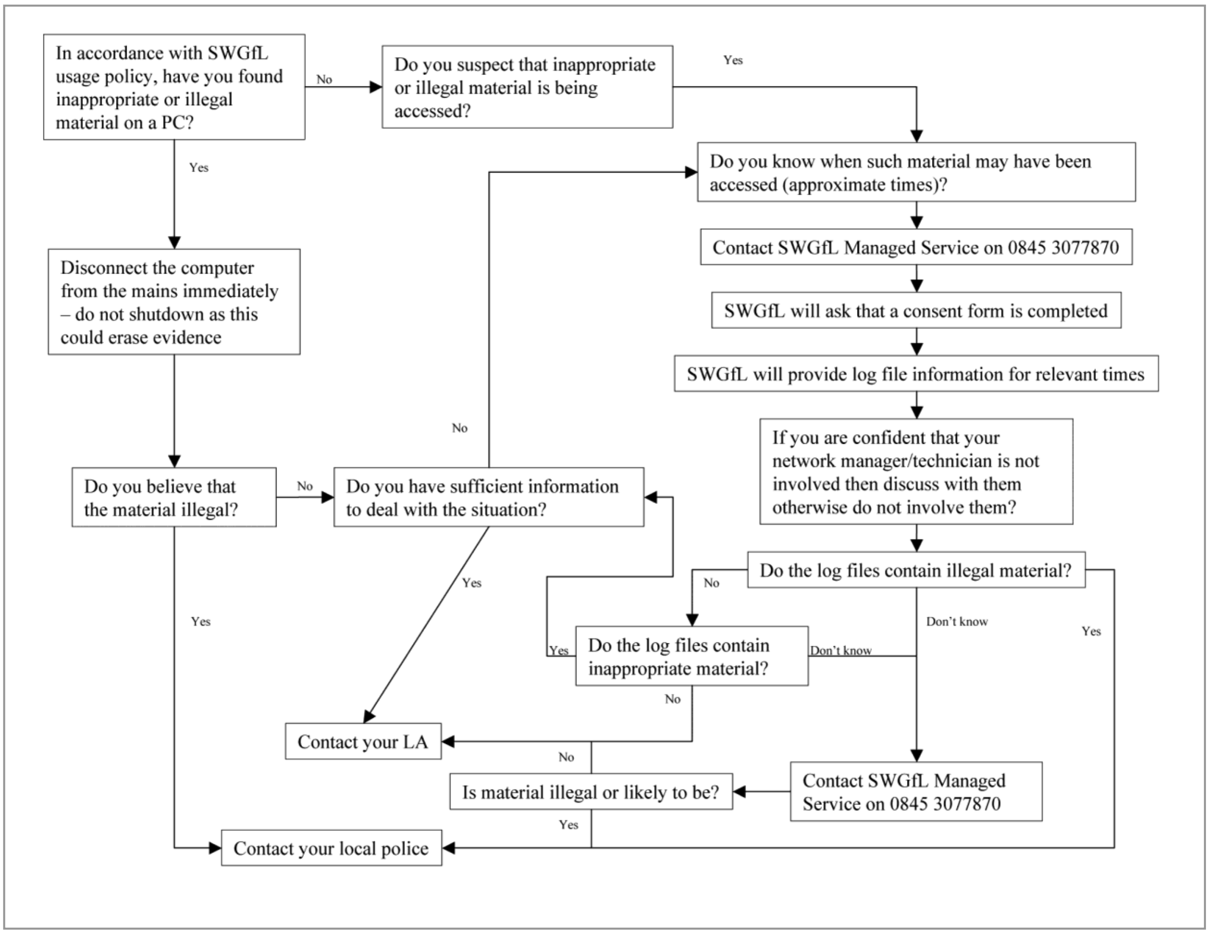
- Staff should not use social networking sites to seek to influence pupils regarding their own political or religious views or recruit them to an organisation of this kind using their status as a trusted adult to encourage this

All communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. Staff are strongly advised, in their own interests, to take steps to ensure that their on-line personal data is not accessible to anybody who they do not want to have permission to access it. For example, they are advised to check the security and privacy settings of any social networking site they subscribe to and set these to maximum. For further information, see the safer internet website http://www.saferinternet.org.uk/ and the South West Grid for Learning Resources http://www.swgfl.org.uk/Staying-Safe

Responding to Incidents of Misuse
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:
If any apparent or actual misuse appears to involve illegal activity i.e.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
No
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
Yes
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL “Procedure for Reviewing Internet Sites for Suspected Harassment and Distress” should be followed. This can be found on the SWGfL Safe website within the “Safety and Security booklet”. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Appendix A

E-SAFETY ACCEPTABLE USE AGREEMENT
FOR THE INTERNET, E-MAIL AND SCHOOL ICT NETWORK & EQUIPMENT

All members of Staff

I understand that I must use school owned ICT systems in a responsible way (whether at school or offsite), to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, wherever possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

- I will ensure that access will only be made via my authorised account, using my own username and password, which will be changed at least every two terms.

- I will ensure that the school's ICT equipment and network are treated with due care, and not tampered with. I will report technical problems to the SLT / Head teacher or ICT technician via the log book.

- I understand that I may only load or download software on to my school laptop, a school computer/network if I have first gained permission from the school's ICT Technician or the Headteacher.

- I understand that the use of the internet on the school network must be related to my professional duties only.

- I understand that accessing (including viewing or showing others) websites on the school network or on school owned ICT equipment which contain inappropriate or illegal materials is strictly forbidden. Such action will lead to the school's disciplinary procedures being instigated and may result in my dismissal.

- I understand that the downloading or printing of materials from websites on the school network or on school owned ICT equipment which contain inappropriate or illegal materials is strictly forbidden. Such action will lead to the school's disciplinary procedures being instigated and may result in my dismissal.

- I understand that creating, circulating, viewing, showing to others and/or forwarding inappropriate, illegal or defamatory material, via e-mail or uploading to websites, is strictly forbidden. Such action will lead to the school's disciplinary procedures being instigated and may result in my dismissal.

- I understand that e-mailing from the school network beyond the school will be through my school Microsoft 365 account. I understand that the use of my personal e-mail during school contact hours is prohibited.

- I understand that I am responsible for all e-mails sent, and for contacts made to those who may then e-mail back into the network.

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

    - I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

    - I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have opinions that are different from my own.
    - 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 photographic images. I will **not** use my personal equipment to record these images, unless I have explicit permission from the Headteacher to do so; all such images will be deleted promptly after use and will not be stored on personal equipment. When these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
    - I will not access chat and social networking sites in school or on school owned systems, and will ensure that if I access such sites out of school I will not cause reputational damage to the school.
    - I will only communicate with pupils and parents/carers using official school systems and will ensure that all such communications are professional in tone and manner
    - I will not engage in any on-line activity that may compromise my professional responsibilities.

- I will ensure that unsolicited e-mails and unknown attachments are not opened and are permanently deleted.

- I will activate the "screen lock" when absent from my work station (Control/Alt/Delete > Lock this computer).

- I will ensure that I log-out and close down my workstation at the end of the day.

- I will ensure that my participation in any forum will not breach confidentiality nor cause reputational damage to the school (i.e. ensure that anonymity applies to any opinions expressed).

- I will ensure that my use of ICT will not contravene the Data Protection Act, nor breach confidentiality.

- I will ensure that any documents/equipment/media that I take offsite will be stored safely and securely, and in accordance with school procedures.

- I will ensure that copyright of materials will be respected. If materials covered by copyright are used, I will ensure that the source is acknowledged and I understand that the infringement of copyright law is illegal.

- I understand that the school reserves the right to monitor my internet use, and to examine, copy or delete any files which are held on the network or any other school owned ICT equipment.

- I understand that I have a duty of care to report to the Headteacher, or Chair of Governors, in confidence, if I witness or suspect any inappropriate or illegal activity by any person on the school network or the internet.

I will report to the Headteacher, or Chair of Governors, immediately if:

- **I am concerned about any misuse of the school ICT infrastructure, internet, or e-mail, or the infringement of this policy.**
- **I am concerned that I have unwittingly infringed a rule in this agreement.**

Sanctions

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also to my use of school ICT systems and equipment out of school and my use of personal equipment in school in situations related to my employment by the school.
- I understand that my infringement of the Acceptable Use Policy will be taken seriously.
- I understand that, in cases of serious misuse, I may be subject to disciplinary action that could include dismissal and/or legal action. In the event of illegal activities this will involve the police.

Agreement

I have read and understood this Acceptable Use Policy and agree to abide by it.

Print name ....

Signed .... **Date ....**

APPENDIX B

YATTON FEDERATED SCHOOLS

E-SAFETY

Rules for Acceptable Use of ICT and the Internet – Foundation Stage

Our ICT rules help us to enjoy using computers and they keep us safe.

I can use the computer during free flow and in the ICT Suite.

I will always be very careful with the computers and the ICT equipment when I am using them.

If I am not careful, I will not be able to use the ICT equipment.

I will tell an adult if something comes up on the screen that I do not understand or upsets me.

Signed (child): . . . .

Signed (parent): . . . .

APPENDIX C

YATTON FEDERATED SCHOOLS

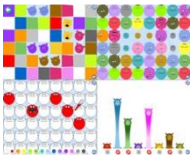
E-SAFETY

Rules for Acceptable Use of ICT and the Internet - Years 1 and 2

Our ICT rules help us to enjoy using computers and they keep us safe.

I will ask my teacher if I want to use the computer.

I will only use programmes or websites that my teacher has told me to use.



I will ask my teacher if I want to do something new or different on the computer.

I will take care of the computers and other ICT equipment.

I will tell an adult if I see something unexpected or that upsets me.

If I break the rules I will not be allowed to use the ICT equipment.

Signed (child): . . . .
Signed (parent): . . . .

APPENDIX D

YATTON FEDERATED SCHOOLS

E-SAFETY

Rules for Acceptable Use of ICT and the Internet - Years 3, 4, 5 and 6

Our ICT rules help us to enjoy using computers and they keep us safe

ICT AT YATTON SCHOOLS

In our school, we believe that ICT and the Internet are very positive and powerful tools which help the teaching you receive and your learning. ICT can make ideas clearer and learning quicker. It can be fun, creative and can be enjoyed both when working by yourself or with others.

We have computers, laptops, exciting software, digital cameras, video cameras, other special ICT equipment, and Internet access which can all be used for teaching and learning. Sometimes your teacher will tell you how to use these tools, and sometimes you will be encouraged to use them creatively by yourself or in a small group.

WHY WE NEED RULES FOR THE ACCEPTABLE USE OF ICT AND THE INTERNET IN SCHOOL

Our school wants you to be able to use ICT and the Internet creatively, responsibly and independently. These rules help you learn what you can do, and what you **must not do**, when using ICT and the Internet in school. They also help you to learn how to behave when out of school. Following the rules protects ICT equipment from damage, and keeps everyone safe and happy.

RULES FOR TAKING CARE OF ICT EQUIPMENT

- I will always be very careful when using any ICT equipment.
  I understand that ICT equipment is fragile and expensive.
  I will carry portable ICT equipment, such as cameras and laptops, carefully with both hands.

- I will not fiddle or play with anything connected to the computer (including headphones).
  I will always leave a computer and ICT equipment as I found it.

- I will only log on to the computer network with my own username and password.
  I will not share my login details with anyone other than my teacher.

- I will not change any settings on the computer without permission from my teacher.
  I will report any warning messages I see on the screen to an adult.
  I will not attempt to by-pass the school's internet filtering system.

- I will not bring CD ROMs or data-sticks into school without teacher permission.
  If I have permission, I will only use them on a computer when my teacher is with me.

RULES FOR KEEPING MYSELF AND OTHERS HAPPY AND SAFE WHEN USING ICT EQUIPMENT, THE INTERNET AND EMAIL

- I will only use the internet and email when given permission and when supervised by my teacher.

- I must ask permission to search the internet.

- I will tell my teacher what I am searching for, and the words I am using to search with.
- I will only look at or download material from the internet that is appropriate to the work I am doing.

- If I see something on the computer or internet that is inappropriate or that upsets me, either at school or at home, I will report it to an adult immediately. Sometimes, this can happen by accident and telling an adult can stop it from happening again.

- I will only send emails to people approved by my teacher.
  I will only send messages that are polite and friendly.
  I will not open emails or attachments from people I do not know.
  I will immediately report to my teacher or my parent any upsetting or bullying messages sent to me at school or at home.

- When using the internet or email, I will not give out my personal details or the personal details of anyone I know at school or at home. (This includes: full names, date of birth, house addresses, email/msn addresses, telephone numbers, name of my school, photos of myself, friends or family, banking details, diary dates).

- I will not attempt to use instant messaging or social networking sites at school.
  These sites are blocked by the school's filter.

- I will never arrange to meet a stranger through the internet or email.
  I will tell my teacher or my parent, if a stranger asks me to meet them.

- On a computer or when using the internet at either school or home, I will not: create, show to others on screen, photocopy, send, forward/pass on any material that would offend, upset or bully other children or adults. (This includes text, pictures, photos, video clips, animations, sound files or any other media).
  I understand that the school takes very seriously the cyber-bullying of any child or adult and must take strong action against it.
  I understand that writing or sending hateful / threatening messages which upset others is illegal.

- I will not upload any material on to the internet without my teacher first checking the content and giving me permission.

- I will respect the copyright of any material posted by others on the internet. If I use information from a website in my own work, I will type the web address on my work.

- I will not break the school's copyright by using the school logo, letterhead, or any other material produced by the school on paper, its network or website without permission.

- I will only use school digital and video cameras when given permission and when supervised by my teacher.
  I will only take appropriate photos or video clips of others or myself.
  I will respect the photos or video clips I have taken of others, and only use these in my work at school.

Mobile Phones

- The school discourages children bringing mobile phones (or other hand held devices) into school. I understand that mobile phones can only be brought to school with my parent/carer's permission.
  I understand that I will need to give my phone in daily to my teacher.
  I understand that if I breach the guidelines of this agreement in respect of my mobile phone, it may be confiscated and I may be banned from bringing a phone to school.
  I will not give the telephone numbers for any of my friends to other people without first asking their permission.
  I understand that everything I create or look at on a computer leaves a "digital footprint" that can be traced.
  I understand that the school monitors my use and can check my computer files and the websites I visit at any time.

TELL AN ADULT WHO WORKS IN SCHOOL STRAIGHT AWAY IF:

- You are worried about anything to do with the Internet or ICT;
- You are worried that you may have broken a rule.

THE ADULT WILL LISTEN TO YOU AND HELP SOLVE YOUR PROBLEM

IF I BREAK THE RULES:

I understand that if I break these rules on purpose one or more of the following will happen:

- I will receive a verbal warning;
- School sanctions may apply;
- I will not be able to use a computer or ICT equipment for a period of time set by my teacher;
- If it is serious, I will be required to speak with Miss Keeble about my behaviour, and my parents/carers will be informed;
- If it is very serious, Miss Keeble will have to act immediately and ask my parents/carers to come into school. At this meeting, my behaviour and the sanctions which may need to be taken will be discussed. If it is **extremely** serious and I have broken the law, a police officer will have to be present at the meeting.

PUPIL AGREEMENT

Name: ……………………………………………….

I agree to keep these rules for the acceptable use of ICT and the Internet at Yatton Junior School.

I understand the sanctions that will be used by the school if I break these rules.

Signed (pupil) ……………………………………………………… **Date ……………………………….**

Signed (Parent/carers) ………………………………………. **Date ……………………………….**

APPENDIX E

YATTON FEDERATED SCHOOLS

ACCEPTABLE USE AGREEMENT FOR THE INTERNET, E-MAIL

AND SCHOOL ICT NETWORK & EQUIPMENT

Volunteers, Visitors and Community Users

- Mobile phones or iwatches must not be used when working with or supervising children. Use of personal devices can only be used in the staff-room or outside of the school building.

- Children should only use the Internet supervised, and all web links checked prior to the lesson.

- Access to the network should only be made through your authorised account using your own username and password. This should be kept secret by yourself and the network administrators.

- Use of the Internet on the school network during school contact hours must be for your professional duties only. At all other times internet use must be appropriate, and should not include financial transactions.

- Accessing (including viewing or showing to others) websites on the school network or on school owned ICT equipment which contain inappropriate or illegal materials is strictly forbidden and could result in action being taken against you.

- Downloading or printing material from websites on the school network or on school owned ICT equipment which contain inappropriate or illegal materials is strictly forbidden and could result in action being taken against you.

- Creating, circulating, viewing, showing to others and/or forwarding inappropriate, illegal or defamatory material, via email or uploading to websites, is strictly forbidden and could result in action being taken against you.

- Confidentiality of all material on the school network must be respected.

- Digital photos and moving images of children should only be taken as part of school life and learning activities and **NEVER** on your own personal camera, phone or mobile device.

- Digital photos or moving images of children should be stored in a labelled folder on staff laptops or the school network.

- Volunteers, students and supply staff must ask permission from their school based supervisor, and temporary teaching and non-teaching staff from the Headteacher, if they wish to use digital images of children from Yatton Schools beyond the school.

- Copyright of materials must be respected. Infringing copyright law is illegal.

- If you have used in your own teaching resources links to images, text and other material which is covered by copyright, then the source(s) must be acknowledged.

- All adults in school have a duty of care to report to the Headteacher, or Chair of Governors, in confidence, if they have witnessed or suspect any inappropriate or illegal activity by any person on the school network or the internet.

Report to the Headteacher, immediately if:

- **you are concerned about anything to do with the school ICT infrastructure, internet, or email.**
- **you are concerned you have unwittingly infringed a rule in this agreement.**

In cases of serious misuse legal advice would have to be taken which could lead to action being taken against you including legal action.

Agreement

I have read and understood this Acceptable Use Agreement and agree to abide by it.

Name : **……………………………………………………………………………………………………..**

Signed: **……………………………………………………..** ***Date:*** **…………………………**

Appendix F – Microsoft Teams Communication to Parents

Safeguarding and Rules

Keeping your child safe and happy is always a high priority so the school staff will keep a close eye on all chat and communication on Teams to ensure it is kind and respectful. Children will be expected to follow the rules of the school – SAFE, READY and RESPECT online. We will all need to follow these guidelines to ensure that it is a good session for everybody involved:

School Staff will:	Parents/ Carers will:
• Provide groups only live contact or 1:1 where this has been planned and approved by the SLT • Provide contact whilst against a neutral background • Wear suitable clothing • Record the live sessions so that if any issues were to arise, the video can be reviewed. These recording will be held securely on the school cloud network. • Use professional and appropriate language. • Use Microsoft Teams on the school's platform. • Log the length, time, date and attendance of any sessions held. • Communicate through any live platform from school email addresses to school email addresses only. Staff will never use private addresses to correspond with students or parents. • Invite each student to attend any live session as pre planned via their Microsoft Teams account. • Abort the session or remove a student should there be any unwanted behaviour or conduct and will report this to the school and parents as necessary.	• Read the guidance below with their children and make sure that they understand the rules. • As much as possible allow children to take part in any VLE session independently- obviously some technical assistance for younger pupils may be required but sessions will be more beneficial if children can interact with their Home Learning Teacher directly rather than parents doing this. • Wear suitable clothing if the chances are they will be passing within screenshot whilst moving around their household. • Ensure their child is located in a communal area of the house. Where parents feel that they are best located in a room on their own, the door should remain open and within earshot of an adult. • Use appropriate language only, even if communicating with another member of the household. This includes gestures and other body language. • Not record, screenshot or otherwise the session as this will breach the Acceptable Use Policy • Raise any concerns they have about any element of the session with the school as soon as possible.

Microsoft Teams and/or Zoom advice for staff

Yatton School’s guidelines for video-streamed/live teaching

- No 1:1s, groups only, or where there is another adult present with the child.
- Sit against a natural background, ensuring that there is nothing in the background that could be controversial.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas.
- Students should be located in a communal area of the house. Where parents feel that they are best located in a room on their own, the door should remain open with the session within earshot of the parent/adult.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Staff must double check that any other tabs they have open in their browser would be appropriate for a child to see, if they are sharing their screen.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the staff getting on with other important school work and the family ‘getting on’ with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided by Yatton/LSP to communicate with students
- Staff should note, the length, time, date and attendance of any sessions held.
- Communication by webcam platforms should be from school email addresses to school email addresses. Staff and students must never use private emails addresses to correspond with each other.
- Staff must not use personal social media for e-learning purposes or communication with students although schools may wish to publish learning materials from school accounts on open social media such as Twitter.

  <u>Safer use of Zoom</u>
- Password protect any meeting
- Use a new meeting room each time (i.e. Do not use the personal meeting ID)
- Do not allow attendees to join before host
- Mute attendees on joining
- Turn screen sharing off
- Set up a 'waiting room'
- Lock your meeting room after you have started
- Do not publicise your meeting's link on social media
- Do not share the screenshot of everyone, especially when it shows the meeting ID
- Try to have someone whose job it is to 'manage the room' and focus just on doing that.
- Tell people what the Plan B is (i.e. if you do have to abort the meeting where will the meeting move to and how can students re-join)