Forres Sandle Manor (Non-Academic) Policy

Policy Title	**E-Safety**
Policy Lead (Appointment (& Initials))	**Deputy Head Pastoral & DSL (LM)**
Date of Last Review	**Sep 2025**
Date of Next Review	**Sep 2026**

E-SAFETY

AIM

This policy aims to protect and educate pupils and staff in their use of technology and provide the mechanisms to intervene and support any incident where appropriate.

SCOPE OF THE POLICY

This policy applies to all members of the Forres Sandle Manor 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 Head teachers, 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 cyberbullying, or other E-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The breadth of issues classified within E-safety is considerable but can be categorised into 4 areas:

- Content: Being exposed to illegal, inappropriate or harmful material.
- Contact: Being subjected to harmful online interaction with other users.
- Conduct: Users personal online behaviour that increases the likelihood of or, causes harm.
- Commercialism: Being exposed to advertising and marketing schemes, which can also mean inadvertently spending money online

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

RELATED POLICIES

This policy should be read in conjunction with the following *DfE documents* and school policies:

- *DfE: Keeping Children Safe in Education*
- *DfE: Sexting in schools and colleges*

- *DfE: Teaching Online Safety in Schools*
- Data Protection Policy.
- Safeguarding and welfare Policy, including Preventing Radicalisation
- Behaviour Management Policy.
- Staff Code of Conduct.
- Staff Handbook.
- Acceptable Use Policy and Children's User Agreement.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school:

The Directors

The Board of Directors are responsible for the approval of the E-safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Director receiving regular information about E-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-safety Director.

The role of the E-safety Director will include:

- Meetings with the DSL
- Monitoring of E-safety incident logs.
- Reporting to relevant Directors committee/meetings.

DSL and Senior Leaders

- **The Head teacher 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 Deputy Head Pastoral and the Head of Digital Learning.
- The Head teacher/Senior Leaders are responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant.
- The Head teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. E-Safety incidents should all be logged on School base to allow for monitoring. Flagged incidents via lightspeed should also be logged on school base and cases closed on lightspeed with notes.
- The Senior Leadership Team will receive monitoring reports from the Deputy Head Pastoral.
- **The Head teacher and Senior Leaders are aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff**. *(See Flow chart on dealing with E-safety incidents – included in a later section – '**Responding to incidents of misuse.'**)*

E-safety Co-ordinator (DSL)

- 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.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school ICT technical staff.
- Receives details of E-safety incidents and creates a log of incidents to inform future E-safety developments.
- Meets regularly with E-safety Director to discuss current issues.
- Attends relevant meeting/committee of Directors and Advisors.
- Reports regularly to the Senior Leadership Team.

E-safety Incidents (Pupils) (Deputy Head)

- Receives details of E-safety incidents and creates a log of incidents to inform future E-safety developments.
- Deals with the investigation, action and sanction of any incidents of a serious nature.
- Meets regularly with Head of Digital Learning and Sense Support to discuss current issues and review incident logs.
- Attends relevant meeting/committee of Directors.
- Reports regularly to Senior Leadership Team.

Technician/Technical Staff

The School's Network is managed by the Sense Support Ltd. They are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school has a robust and secure network taking into account best practice from government and other guidance.
- Users may only access the school's networks through a properly enforced password protection policy.
- That the Internet connections filter is working and monitored. Currently FSM are using Lightspeed with separate censoring policies for staff and children dictated by the configurations of the software. Lightspeed Alert provides PREVENT and self-harm compliance.
- That they keep 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/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Deputy Head for investigation/action/sanction.
- That monitoring software/systems are implemented and updated.

Teaching and Support Staff

- 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).
- They report any suspected misuse or problem to the Deputy Head, Head of Digital Learning and Network manager for investigation.
- Digital communications with students/pupils (email/voice) 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.
- Ensure pupils understand and follow the school E-safety and acceptable use policy.
- Ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extended school or extra-curricular activities and Boarders' free time.
- They are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and 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 processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

They should be trained in E-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

  (NB. It is important to emphasise that these are safeguarding issues, not technical issues. Simply that the technology provides additional means for child protection issues to develop. At FSM the roles of Designated Safeguarding Lead and E-safety Officer have been combined.)

E-safety Committee

Members of the E-safety Committee will assist the Deputy Head with:

- The production/review/monitoring of the school E-safety policy and other related documents.
- The implementation of appropriate levels of filtering.

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, (as explained in Computing lessons) which they will be expected to sign before being given access to school systems (no signature required at Key Stage 1.)
- Have a good 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, if related to their membership of the school.
- Should be aware of their digital footprint and online reputation.

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 some 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 opportunities to help parents understand these issues through *parents evenings, newsletters, letters, website and information about national/local E-safety campaigns/literature.* See also *E-safety advice for Parents*

A copy of the Pupil Acceptable Use Guidelines will be sent annually to parents.

POLICY STATEMENTS

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

E-safety education will be provided in the following ways:

- A planned E-safety programme is provided as part of ICT/Lifeskills and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key E-safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities, including visiting speakers. – see appendix 9

- Key E-safety messages are also reinforced through SMART posters and the 'Acceptable Use of Digital Communications, the ICT Room and Network'- Guidance for Children – See Appendix 2.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils are helped to understand the need for the student/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 to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

Education – Parents/Carers

Some parents and carers have a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. "There is a generational digital divide," (Byron Report.) The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website.
- Parents' evenings.
- Reference to suitable websites.

Education and Training

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

- A planned programme of E-safety training is carried out on a rolling program via INSET training sessions.
- All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Policies.
- The DSL and other key staff will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by Government/LA and others.
- This E-safety policy and its updates will be presented to and discussed by staff in INSET days.
- The DSL and network manager will provide advice, guidance and training to individuals as required.

Training Directors

Directors should take part in E-safety awareness sessions. This is of particular importance for the Safeguarding Director (Chair of the board). This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Director Association or other relevant organisation.
- Participation in school training/information sessions for staff or parents.

Technical – Infrastructure/Equipment, Filtering and Monitoring

FSM will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible, and that the policies and procedures approved within this policy are implemented. FSM will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the standards of E-safety and take into account any relevant Local Authority or expert 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.
- All users (KS2 and above) will be provided with a username and password by the Head of Digital Learning and/or Sense IT. Users will be advised to change their password periodically. The “administrator” passwords for the school ICT system, used by Sense IT (or other person) must also be available to SLT upon request.
- Users will be made responsible for the security of their username and password, 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.
- The school has provided enhanced user-level filtering through the use of our ‘Lightspeed’ Filter.
- In the event of the Sense IT (or other person) 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 Interim Headmaster (or other nominated senior leader).
- Requests from staff for sites to be removed from the filtered list will be considered by the Sense IT and if the request is agreed, this action will be recorded.
- Sense IT regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual/potential E-safety incident to the Network Manager.
- An agreed policy is in place for the provision of temporary access of “guests” e.g. trainee teachers, visitors) onto the school system.

- We use ‘Sophos Antivirus’ and ‘Lightspeed’ to protect the school infrastructure and individual workstations.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line, and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be taught about their digital footprint and online reputation.
- Be made aware of the effects on their health and wellbeing (such as the amount of time they spend working on a screen.

Artificial intelligence (AI)

Please see specific AI policy for further information.

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as, smartphones, iPads, games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. FSM chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

BRING YOUR OWN DEVICE (BYOD)

FSM recognises that as technology has changed more pupils have access to Internet capable devices. FSM also recognises that some pupils will gain improved access to the curriculum through these methods than by some more traditional methods.

Devices in the form of tablet computers and laptops may be used in classrooms to aid learning but only with permission from staff.

General Information

Access to FSM wireless network, whether with school-provided or personal devices, is filtered in compliance with the Children's Internet Protection Act (CIPA). Pupils will not have access to any documents which reside on the FSM network from their personal devices. Access to the FSM School wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all school rules. The use of the network also allows IT staff to conduct investigations regarding inappropriate Internet use at any time, by teacher request.

Obtaining access to the network:

All access for non-school IT equipment for staff such as mobile phones, tablets, laptops etc should use the FSMGuest Wi-Fi network. For boarders they will use the separate boarders network. This separate connection is filtered globally at a level suitable for student and adults. The filtering in place is inline with current CIPA guidelines, FSM's own usage policies and what would be considered appropriate for a workplace environment.

Guidelines for Use

- Pupils may only bring in personal devices with the permission of the school.
- Use of personal devices during FSM day is at the discretion of teachers and staff. Pupils must use devices as directed by their teacher.
- The primary purpose of the use of personal devices at school is educational. During the school day, using the device for personal reasons e.g. gaming, gambling or accessing social network sites is not allowed within school and contacting parents, should only take place after permission has been given from a teacher or other member of staff.
- The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class in any way.
- The use of personal devices falls under FSM School's Acceptable Use Policy.
- Pupils shall not use personal devices outside of their classroom, e.g. break and lunchtimes, unless otherwise directed by their teacher e.g. on school visits or activities.
- Pupils shall make no attempts to circumvent FSM's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.

- Pupils shall not create, store or distribute pictures or video of pupils or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

Consequences for Misuse/Disruption (one or more may apply):

- Access to the wireless network will be removed.
- Device taken away for the period.
- Device taken away and kept in the front office until parent picks it up.
- Pupil is not allowed to use personal devices at school.

Serious misuse of Internet or other mobile technology capable devices is regarded as a serious offence within FSM's Behaviour Policy and will be dealt with in accordance with this policy. The police will be advised where inappropriate or illegal content or activity is suspected, reported or identified.

See Appendix 3: *Guidelines for the safe and appropriate use of digital communications'*

School Liability Statement

Pupils bring their devices to use at FSM School at their own risk. Pupils are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

FSM School is in no way responsible for:

- Personal devices that are broken while at school or during school-sponsored activities.
- Personal devices that are lost or stolen at school or during school-sponsored activities.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
- Parents should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal ICT device in the event of loss/damage to the device.

Use of Digital and Video Images – Photographic, Video

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 should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website as per the list maintained in the School Office.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off", or locked at the end of any session in which they are using personal data or time that they leave the room.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

	Staff and other adults					Pupils			
Communication Technologies	Allowed	Allowed at certain times with restrictions in place	Allowed for selected staff	Not allowed		Not Allowed	Allowed at certain times	Allowed with staff permission	Allowed by Boarding pupils
Mobile phones may be brought to school	✓							✓	✓
Use of mobile phones in lessons				✓		✓			
Use of mobile phones in social time	✓						✓		✓
Taking photos on personal mobile phones or other camera devices				✓					✓
Use of hand held devices e.g. PDAs, PSPs		✓							✓
Use of personal email addresses in school, or on school network		✓							✓
Use of school email for personal emails		✓					✓		
Use of chat rooms/facilities			✓			✓			✓
Use of instant messaging		✓							✓
Use of social networking sites		✓				✓			
Use of blogs		✓						✓	

** Use of technology in the boarding house is closely monitored by staff and children only given access to their personal technology with staff permission at certain times.

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), must be professional in tone and content. *These communications should only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.*
- Pupils should be taught about 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.
- 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

FSM believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

Staff should also be aware that disclosing the Wireless Network codes to pupils will be deemed a disciplinary offence. It is of the utmost importance that the wireless access codes are not written down or left anywhere that could be found by a child.

The school policy restricts certain internet usage as follows:

		Acceptable	Acceptable at certain times	Accepted for nominated users	Unacceptable	Unacceptable and illegal
Users Actions **When in school or using school devices outside of school, users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:**	Child sexual abuse					✓
	Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	Adult material that potentially breaches the Obscene Publications Act in the UK					✓
	Criminally racist material in the UK					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Promotion of racial or religious hatred				✓	
	Threatening behaviour, including promotion of physical violence or mental harm				✓	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by 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					✓	
On-line gaming (educational)			✓			
On-line gaming (non-educational)				✓		
On-line gambling					✓	
On-line shopping/commerce				✓		
File sharing				✓		
Use of social networking sites				✓		
Use of video broadcast				✓		

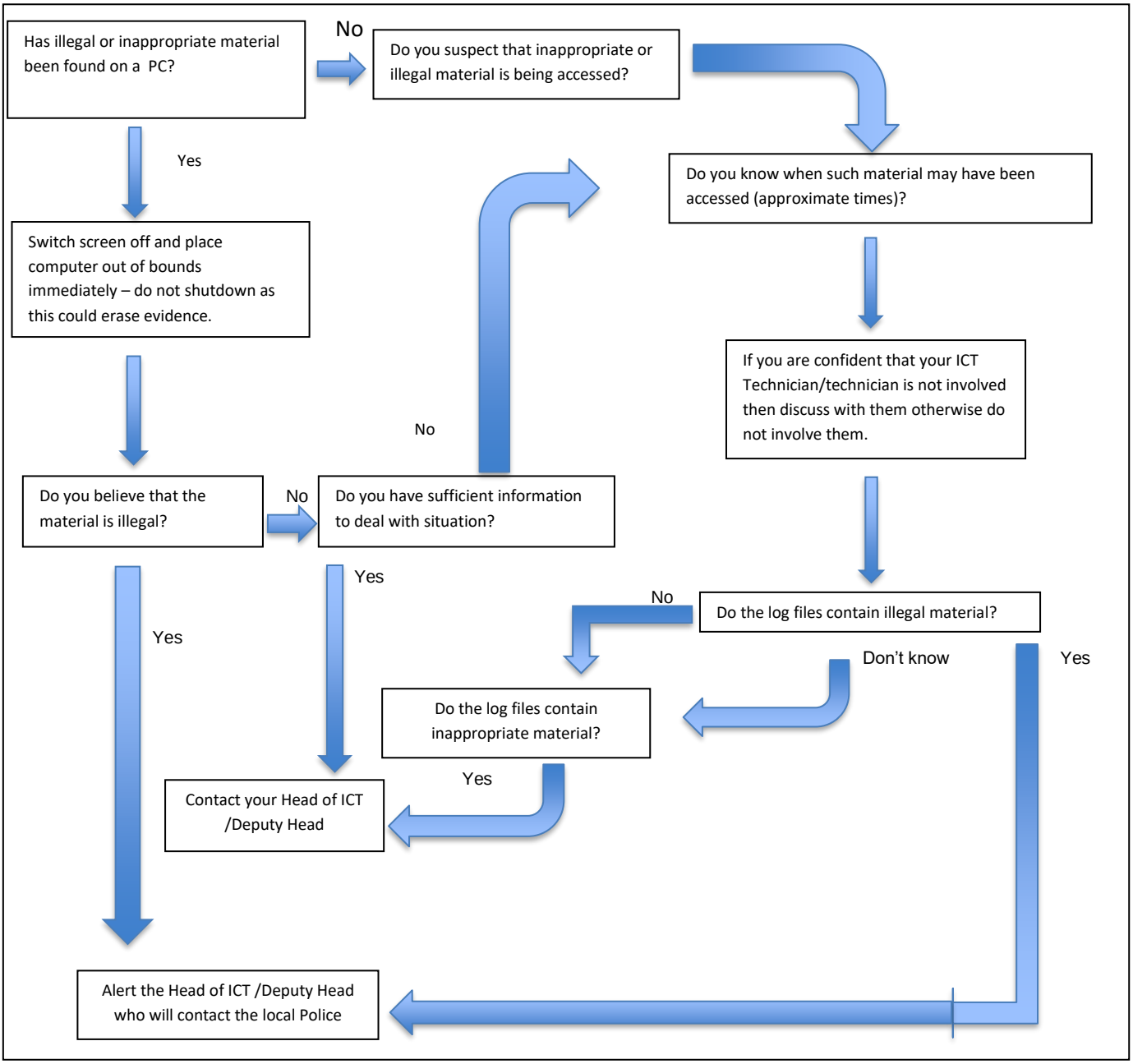
Responding to Incidents of Misuse

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.**

Then the flow chart below 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.



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.

This guidance recommends that more than one member of staff is involved in the investigation.

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 as follows:

Students/Pupils Actions/Sanctions

	Refer to class teacher/tutor	Refer to Deputy Head	Refer to Headmaster	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓					
Unauthorised use on non-educational sites during lessons	✓						✓	✓	✓
Unauthorised use of mobile phone/digital camera/other hand held device	✓	✓				✓	✓	✓	✓
Unauthorised use of social networking/instant messaging/personal email	✓					✓	✓	✓	✓
Unauthorised downloading or uploading of files	✓				✓		✓	✓	
Bringing into school, playing or watching age inappropriate games/videos/films	✓	✓				✓	✓	✓	✓
Allowing others to access school network by sharing username and passwords		✓			✓		✓		
Attempting to access or accessing the school network, using another student's/pupil's account	✓	✓			✓				✓
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓				✓		✓
Corrupting or destroying the data of other users	✓	✓							✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓			✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓		✓	✓	✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓			✓	✓			
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓	✓		✓	✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓	✓			✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓	✓						✓

Staff **Actions/Sanctions**

Incidents:	Refer to Ops Dir / Deputy Head	Refer to Headmaster	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓				
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email	✓	✓				✓		
Unauthorised downloading or uploading of files	✓					✓	✓	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓					✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓					✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓						✓
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	✓	✓				✓	✓	✓
Actions which could compromise the staff member's professional standing	✓	✓				✓	✓	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓						
Using proxy sites or other means to subvert the school's filtering system	✓				✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓				✓		✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓						✓
Breaching copyright or licensing regulations	✓	✓						✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓						✓

Appendix 1

ACCEPTABLE USAGE

INTRODUCTION

This Policy has been developed in order to provide guidelines relating to the acceptable use of the internet and other digital communications related technology by pupils and staff. This policy is to dove-tail with the School's Child Protection and Safeguarding Policies, E-safety, Anti-bullying, Cyber Bullying and Searching Pupils Policies.

All members of the school community will be made aware of the policy. The Acceptable and unacceptable usage sheets are to be supported by sign-up acceptance by users of the school IT facilities.

The policy will be reviewed and amended annually, with particular regard to the expected developments in the operational use of the system, and by reference to the development of recognised best practice.

PURPOSE OF ACCEPTABLE USE POLICY

This policy provides guidance about acceptable use, with regards to the internet, and of any electronic or digital technology by FSM's pupils and staff, including but not limited to: computers, wireless computers, mobile phones, PDAs, Kindles, digital cameras and games consoles. The policy also describes the standards that users are expected to observe when using these facilities and ensures that users are aware of the legal consequences attached to inappropriate use of the facilities.

The policy is designed to advise users that their usage of facilities for internet access will be monitored and, in some cases, recorded. Usage of internet facilities in breach of the policy may lead to appropriate disciplinary action being taken.

The policy also specifies the actions that the School will take in the investigation of complaints received from both internal and external sources, about any unacceptable use of the internet and related technology.

SCOPE

This policy applies to the use of the internet and any related equipment provided by the school or accessed for personal use, as well as pupils' personal equipment that is brought into the school environment including school events off site. The Policy is applicable to members of staff, pupils and other authorised users of School IT facilities.

APPROPRIATE AND PROPER USE

FSM School supports the appropriate and proper use of the Internet, email, and related services and facilities that the School provides for its staff, pupils and other

authorised users. Pupils are required to sign that they have read and understood the Acceptable Use Policy.

ACCEPTANCE OF POLICIES AND REGULATIONS

It is a condition of use of IT and email facilities provided by FSM School, by a member of staff, pupil or other authorised person, that the user agrees to be bound by the relevant School Policies and Regulations.

MONITORING ARRANGEMENTS

FSM School will maintain appropriate monitoring arrangements in relation to all Internet, email and related services and facilities that it provides, and the School will apply these monitoring arrangements to all users without prior notification or authorisation from users.

These arrangements may include checking the contents of, and in some instances recording, email messages for the purpose of:

- Protecting the pupils at the School.
- Ensuring the security of the system and its effective operation.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Making sure there is no unauthorised use of the School's time.
- Ensuring that inappropriate, restricted or blocked websites are not being accessed by employees.
- Making sure there is no breach of confidentiality.
- Establishing the existence of facts relevant to the business.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- Preventing or dealing with cases of cyberbullying.

FSM may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of this Policy. These monitoring arrangements will operate on a continual and continuing basis, with the express aim of monitoring compliance with the provisions of the School's Acceptable Use Policy and for the purposes outlined above as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Boarders are given specific guidance on safe use of technology in the Boarding House (Appendix 3.)

CONDUCTING A SEARCH OF AN ELECTRICAL DEVICE

The school has the right to examine any data or files on a device if they think there is good reason to do so. Following an examination, if the person has decided to return

the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The member of staff must bear in mind the following guidance issued by the Secretary of State when determining what is 'good reason' for examining or erasing the contents of an electronic device:

In determining 'good reason' to examine or erase the data or files the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

Any technology used personally by boarding pupils may be subject to regular checks by boarding staff for potentially harmful or inappropriate material. Boarders are given specific guidance on safe use of technology in the Boarding House (Appendix B.)

See also Searching Pupils Policy.

DISCLAIMERS

FSM may arrange for an appropriate disclaimer to be appended to all email messages that are sent to external addresses from the School, in order to provide necessary legal protection.

ACTION IN THE EVENT OF A BREACH OF THE STANDARDS OF ACCEPTABLE USE

In circumstances where there is assessed to be a breach of the standards of acceptable use, the School will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials. This action will be taken in accordance with the normal managerial arrangements, and will typically involve liaison between the appropriate members of the Senior Leadership Team and Directors. Indications of non-compliance with the provisions of the Acceptable Use Policy will be investigated, as appropriate, in accordance with the provisions of the School's Disciplinary Procedures, as applicable to staff and pupils.

Subject to the findings of any such investigation, non-compliance with the provisions of the Acceptable Use Policy will lead to appropriate disciplinary action, which could include dismissal on the grounds of gross misconduct. Furthermore, publication of some materials may not only amount to a disciplinary offence, but also a criminal offence, in which case the issue will be reported to the police for them to take appropriate action.

APPROPRIATE USE OF THE SCHOOL PROVIDED SERVICES AND FACILITIES

The main purpose for the provision by the School of IT facilities for email is for use in connection with the teaching, learning, research, and approved business activities of the School.

IT facilities provided by the School should not be used:

- For personal use, other than as specified below.
- For the transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk-mail of any kind, to other user organisations, or to organisations connected to other networks, other than where that material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- For the unauthorised transmission to a third party of confidential material concerning the activities of FSM School.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For the deliberate unauthorised access to services and facilities accessible via the School Network.
- For the unauthorised provision of access to School services and facilities by third parties.
- For activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users, especially during teaching hours.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.

GENERAL STANDARDS OF USE

IT facilities provided by the School for email should not be used:

- For the creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs. FSM School is committed to fostering a learning and working environment free of discrimination where everyone is treated with dignity and respect. See also ***Safeguarding Policy (including Prevent)***
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called 'flaming' i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For criticising individuals, including copy distribution to other individuals.

- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages, i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the School into disrepute.

School Management will exercise its discretion in judging reasonable bounds within the above standards for acceptability of material transmitted by email.
The School regards the declaration of standards, as described above, to be particularly important. They reflect the values and beliefs of FSM School.

PREVENTING THE SPREAD OF MALICIOUS SOFTWARE (VIRUSES)
Users of School IT facilities must take all reasonable steps to prevent the receipt and transmission by email of malicious software e.g. computer viruses.

In particular, users:
- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access School IT facilities.
- Must not open email file attachments received from unsolicited or untrusted sources and should be aware of email addresses that closely resemble those they recognise but are in fact not.

PERSONAL USE
The School permits the use of its IT facilities for email by staff, pupils and other authorised users for personal use, subject to the following limitations:
- A level of use that is reasonable and not detrimental to the main purpose for which the facilities are provided.
- Priority must be given to use of resources for the main purpose for which they are provided.
- Personal use must not be of a commercial or profit-making nature, or for any other form of personal financial gain.
- Personal use must not be of a nature that competes with the School in business.
- Personal use must not be connected with any use or application that conflicts with an employee's obligations to FSM School as their employer.
- Personal use must not be connected to any purpose or application that conflicts with the School's rules, regulations, policies and procedures.
- Personal use must comply with the School's policies and regulations, in particular the Acceptable Usage Policy.
- In relation to the personal use of School IT facilities for email, if users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance, in the case of members of staff, of the Senior

Leadership Team, and in the case of pupils, of their tutor, teacher or a Resident member of staff.

Pupils are given guidance by the Head of social networking sites. (Appendix 2) Further to this, boarding pupils are also given guidance specific to the use of the internet and related technology in the Boarding House. (Appendix 3)

All pupils in years 3 - 9 are asked to sign a sheet confirming that they have read and understood the rules regarding the appropriate use of the internet (Appendices 4 & 5).

Further guidance on E-safety is given through the schools PSHE/lifeskills curriculum and through visiting speakers. Parents are also given the opportunity to attend such talks. Parents are also sent an advice sheet with regards their children and Internet use*.*

LEGAL CONSEQUENCES OF MISUSE OF EMAIL FACILITIES

In a growing number of cases involving the civil or criminal law, email messages (deleted or otherwise) are produced as evidence in a permanent written form.

There are a number of areas of law which apply to use of email and which could involve liability of users or the School. These include the following:

- **Intellectual property**. Anyone who uses email to send or receive any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them.
- **Obscenity**. A criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly, the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child. Even viewing such material on a website creates a copy on the hard drive which the law views as creating an image.
- **Defamation**. As a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the email and may lead to substantial financial penalties being imposed.
- **Data Protection**. Processing information (including photographs) which contains personal data about individuals requires the express written consent of those individuals. Any use of personal data beyond that registered with the Data Protection Commissioner will be illegal.
- **Discrimination**. Any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Sex Discrimination Act 1975, the Race Relations Act 1976 or the Disability Discrimination Act 1995 where it involves discrimination on the grounds of sex, race or disability.

The above is only designed to be a brief outline of some of the legal consequences of misuse of email facilities.

INVESTIGATION OF COMPLAINTS

The School will investigate complaints received from both internal and external sources, about any unacceptable use of email that involves School IT facilities.

The investigation of facts of a technical nature, e.g. to determine the source of an offending email message, will be undertaken by the Senior Leadership Team in conjunction with other departments as appropriate.

Where there is evidence of a criminal offence, the issue will be reported to the police for them to take appropriate action. The School will co-operate with the police and other appropriate external agencies in the investigation of alleged offences.

In the event that the investigation of the complaint establishes that there has been a breach of the standards of acceptable use, then action will be taken as described in this Policy.

Appendix 2 – Guidance for Children

ACCEPTABLE USE OF DIGITAL COMMUNICATIONS, THE ICT ROOM AND NETWORK

Pupils may use the ICT room, internet and other digital communications subject to the conditions laid down under "Network Etiquette." These rules include but are not limited to:

- Use during free time.
  - Pupils may use the ICT room during free time with direct supervision by duty officers.
  - Pupils may only use computers in other classrooms with the permission and direct supervision of a teacher.
- Pupils are responsible for good behaviour in the ICT Room. General school rules apply.
- Be polite – never send or encourage others to send abusive messages.
- Do not log-on to the network or send e-mails from another users account.
- Use appropriate language – users should remember that they are representatives of FSM on a global public system. Illegal activities of any kind are strictly forbidden.
- Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
- Password – do not reveal your password to anyone. If you think someone has learned your password then contact the IT Department staff.
- Pupils may not bring in, play or watch age inappropriate material at FSM.
- Pupils will not be allowed access to public or unregulated chat rooms. Pupils should only use regulated educational chat environments.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the IT Department staff.
- Do not attempt to interfere with FSM's IT system (e.g. hacking)
- Users should log out when their session has finished.
- Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.
- Do not load non-approved software as this could cause major problems.
- Do not attempt to visit sites that might be considered inappropriate. All sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- Watch for accidental access to inappropriate materials and report to the ICT Department staff.

- It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.
- Files held on the school's network will be regularly checked by the ICT Department staff.
- School work and email communication with family members will be given priority over recreational use
- *Note: Users' personal responsibility is necessarily limited by age in Early Years and Key Stage 1 especially.*

NETWORK USE POLICY FOR PUPILS

- The e-mail use policy is displayed in the ICT Room and is taught to Year 3 pupils and above when appropriate within the curriculum.
- These rules help to keep everyone safe.
- Only use your own network login and password, which is secret.
- Only look at or delete your own files.
- Do not bring software or disks into school without permission.
- Only e-mail people you know, or with a teacher's permission.
- The messages you send must be polite and sensible.
- Never give your home address or phone number, or arrange to meet someone.
- Ask permission before opening an e-mail or an e-mail attachment sent by someone you do not know.
- Do not use Internet chat.
- If you see anything you are unhappy with or receive messages you do not like, tell a teacher immediately.
- Understand that the school may check your computer files; the Internet sites you have visited and email you have sent and received.

SANCTIONS

- Any pupil failing to comply with the acceptable use guidelines will receive a temporary or permanent ban from use outside lesson times of all forms of digital communication.
- Additional disciplinary action may be taken as required in accordance with the school Behaviour management Policy and Anti Bullying policies.
- Certain types of Internet and Email abuse are illegal and in such cases appropriate action will be taken following guidance from the appropriate agency or the Police.

Should you have any concerns or questions with regards digital communications, the ICT room or network and their use, please see SLT or Head of Digital Learning.

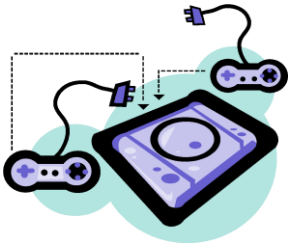
Forres Sandle Manor School
Guidelines for the safe and appropriate use of digital communications.

- Mobile phones, iPods, iPads and games consoles etc. are to be handed into matrons/staff on the first evening that they are brought into school.
- Devices can be collected from the cupboard at the given times each evening but must only be used during free time. Times of use are clearly explained to pupils and parents.
- No electricals, with the exception of E-readers, may be used in the dormitory itself.
- Photos or film must never be taken in the dorms or wash/changing areas
- E-readers must also be handed in each evening but may be collected in the morning if they are to be used in school
- Age inappropriate games/films/videos are not allowed in school.

Pupils are reminded of the School's ICT policy:

a) Tell a teacher straight away if you find any information or pictures that are unpleasant, rude, racist, threatening, worrying or make you feel uncomfortable or unhappy. Also tell a teacher if you receive unpleasant or unwanted messages from anyone; including other pupils.

b) Do not turn the device off. Turn the monitor off and notify your teacher immediately without showing other pupils the offensive materials.



Pupil's must **not** use offensive language or use devices to:

i. Harass, insult or attack others,
ii. Take or distribute pictures of another individual without their permission
iii. Send, receive or display offensive messages or pictures,
iv. Copy or reproduce material in violation of copyright laws. (N.B. Simply downloading material to a local cache can violate copyright.
v. Send messages to teachers unless they have been asked to.

Children are advised to PIN lock their equipment but pupils understand, when asked, they will show the content of the equipment to a member of staff. Failure to comply will result in the equipment being sent home to be checked by parents and being banned from school for the period of half a term.

Sanctions

1. Any pupil failing to comply with the acceptable use guidelines will lose the use of their device on a temporary or permanent basis depending on the seriousness of the breach of trust
2. Additional disciplinary action may be taken as required in accordance with school Behaviour Management Policy and Anti Bullying policy
3. Certain types of Internet and Email abuse are illegal and in such cases appropriate action will be taken following guidance from the appropriate agency or the Police.

Appendix 4 – *Year 5 - 10 Pupil Acceptable Use Agreement*

Year 5 - 10 Pupil Acceptable Use Agreement

FORRES SANDLE MANOR
FORDINGBRIDGE

This document refers to all Digital communications (including phones, computers, digital cameras, PDAs, E-readers, and gaming machines etc.)

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
If I have any concerns or questions with regards digital communications, the ICT room or network or their use I will see Mr Fairbairn (Head of Computing).

Keeping Safe

- I will not use ICT in school (including my own ICT) without permission.
- I know that the school will monitor my use of the ICT systems and communications.
- I will only use my own user names and passwords which I will choose carefully to protect my identity and I will not share them.
- I will keep my personal details and those of others private.
- I will log off sites and computers when finished.
- I understand that different sites have safety features and use them.
- I will not visit unsafe sites or register for things I am not old enough for.
- I will not try to upload, download or access anything online which is illegal or inappropriate or may cause harm or distress to others.
- I will not try to bypass the filtering and security systems in place on school ICT.
- I will not bring in/play or watch age inappropriate material in school.

Communicating

- I know that I need to be polite and friendly online.
- I know that others may have different opinions and that I should respect them.
- I am careful about what I send in messages and the language I use as I know that messages can be forwarded on to my parents or headmaster.
- I know that people online may not be who they seem.
- I will make sure my teacher / parents know who I communicate with online.
- If I want to arrange to meet an online friend I will tell an adult and take someone with me.
- I will not open messages if the subject field contains anything offensive or if I do not know who it is from.
- I will not use chat and social networking sites.

Research and Fun

- I will use clear search words so that I can find the information I want safely.
- I will double check the information that I find, as some information online may not be truthful.
- I know that some content may not be filtered out.
- I know that school ICT is for learning and I will not use the systems for personal use or fun unless I have permission. This includes making large downloads/uploads, games, shopping and video broadcasting.

Sharing

- I will not access or use any other user's files without their permission and will credit their work if I use it.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

- I know that downloading from fileshares is illegal and that it can lead to viruses which could damage the computer, slow it down and eventually lead to it having to be removed and cleaned.
- I will not take images of anyone in changing rooms or dormitories.
- I will not take or share images of anyone without their permission.
- I will take care about what I publish on the web as I know once published I cannot control what it is used for.

Buying and selling
- I can identify web sites that are trying to sell something.
- I know that I should ask permission if I am buying / selling anything online.
- I know that I should not respond to offers that I have not asked for as they may be scams.
- I will not use someone else's identity to buy things online

Problems
- I will not try to alter computer settings or install programmes unless I have permission.
- I will immediately report any unpleasant or inappropriate material or messages that I see on computer or online.
- I will not damage equipment and will report any damage or faults involving equipment or software, however this may have happened.
- If I receive an upsetting message / e-mail I will not reply but will save it and report it. If it is received via a chat program or posted on a social networking site, I know I should take a screen shot of it so it can clearly be seen in context.
- I know that viruses and other harmful programmes can be sent by e-mail so I will not open any attachments to emails unless I know and trust the person who sent it.

Acceptable Use Agreement Form
I understand that these rules are in place to enable me to use ICT safely

I know that my use of the ICT in school could be monitored to ensure I am behaving in an acceptable way. I also understand the school has the right to examine any data or files on a device if they think there is good reason to do so.

I agree to use ICT by these rules when:
- I use the school ICT or my own ICT (when allowed) in school
- I use my own ICT out of school to use school sites or for school activities

I understand that if I do not follow them the following sanctions may be used:
1. Loss of use of the device/ICT use on a temporary or permanent basis depending on the seriousness of the breach of trust
2. Additional disciplinary action may be taken as required in accordance with school Behaviour and Disciplinary policy and Cyber Bullying policy.
3. Certain types of Internet and Email abuse are illegal and in such cases appropriate action will be taken following guidance from the appropriate agency or the Police.

Appendix 5 – ***Year 3 – 4 Pupil Acceptable Use Agreement***

FORRES SANDLE MANOR
FORDINGBRIDGE

YEAR 3 – 4 PUPIL USER AGREEMENT FORM for the Pupil Acceptable Use Policy

I agree to follow the school rules when using all forms of ICT devices in school.

I will use the ICT devices in a sensible way and follow all the rules explained by my teachers and contained in the 'Acceptable use of Digital Communications, the ICT Room and Network' situated in the IT room and the 'Guidance for the acceptable use of digital communications' posted in the Boarding House.

I agree to report any silly use of devices to a member of staff.

I agree to tell a member of staff if I see any information that makes me feel uncomfortable.

I understand that staff are able to check my device if they suspect I have broken school rules and I agree that if I PIN lock a device, I will unlock it if a member of staff asks me to. If I do not unlock it I understand that the device will be taken from me and passed to my parents.

If I do not follow the rules, I understand that I might not get to use mine, other people's or the school's devices.

Appendix 6 –*Staff Acceptable Use Agreement*

<u>This has been disseminated to staff via a google form link but a hard copy is shown below</u>

Staff (and Volunteer) 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 internet access 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 ICT 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 ICT in their everyday work.

FSM will try to ensure that staff and volunteers will have good access to ICT 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 FSM ICT systems in a responsible way, 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, where possible, educate the young people in my care in the safe use of ICT and embed E-safety in my work with young people.

For my professional and personal safety:

- I understand that FSM will monitor my use of the ICT systems, email and other communications.
- I understand that the rules set out in this agreement also apply to use of FSM ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that FSMs ICT 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 FSM.
- I will follow the FSM Password Security Policy I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (eg on the FSM website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the FSM's policies.

- I will only communicate with pupils using official school systems. On leaving FSM School service, staff members must not contact FSM School pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.
- I am aware of the risks attached to using my personal email address / mobile phone / social networking sites for such communications with parents. Any such communication will be professional in tone and manner.
- I will not use FSM School corporate, service or team logos or brands on personal webspace.
- 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:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- 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 not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not 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, especially during teaching hours.
- 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 School Data Protection Policy. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that the 'Data Protection Policy' requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy 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:

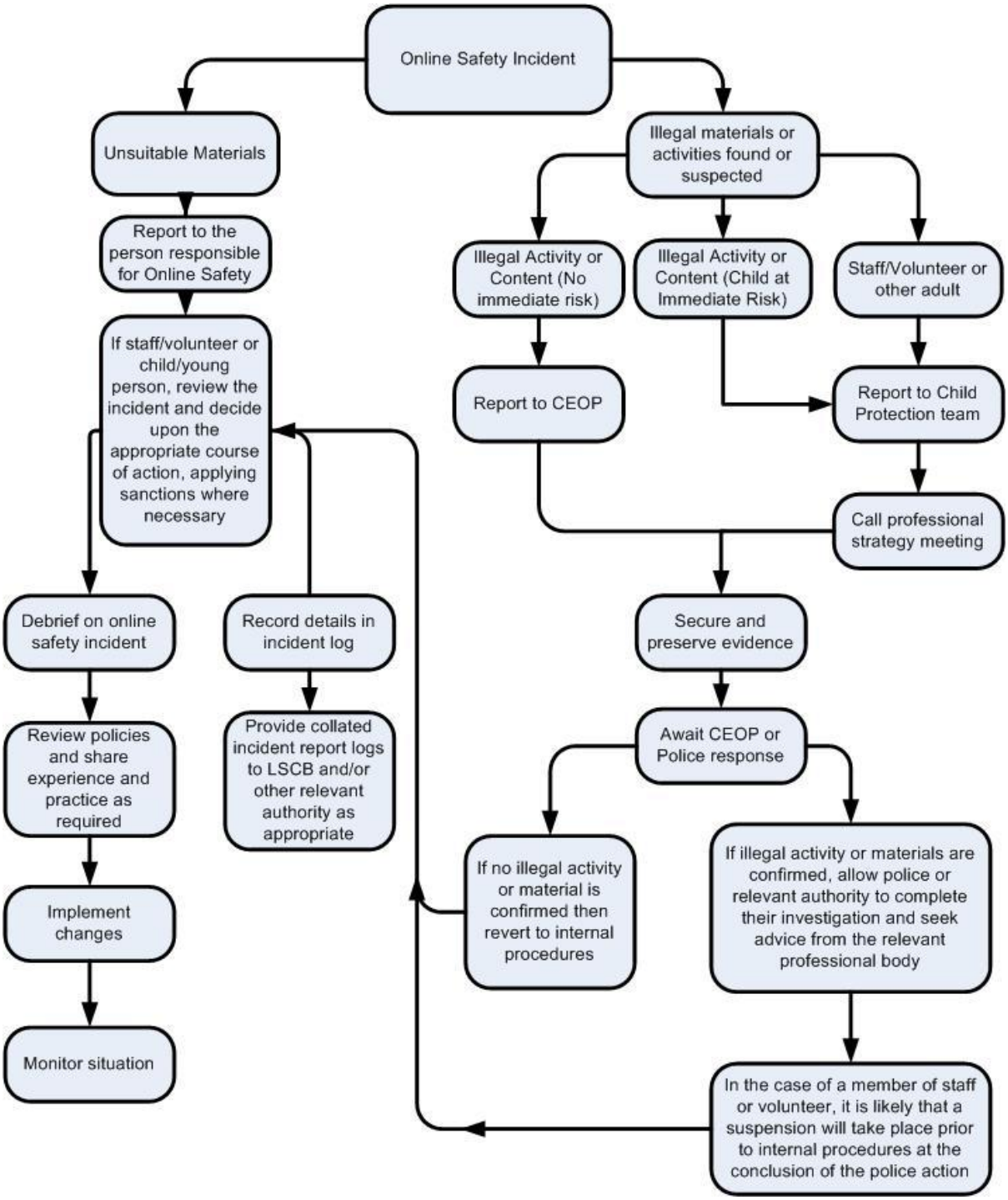
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (inc. music and videos).

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 ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Appendix 7 – Responding to incidents of misuse – flow chart

Responding to incidents of misuse – flow chart



Appendix 8 – Programme of E-safety checks, assemblies and speakers

Termly:

Start of term Boarding house meetings to discuss E-safety guidelines and expectations
E-safety reminders in IT lessons
User agreements checked and signed
Senior & Junior Boarding house meetings – pupil views on E-safety gathered

Annually :

Early ICT lessons of year – E-safety
Early assembly in Autumn term – Who to talk to, bullying, cyberbullying
2nd week in February – E-safety week

Every other year:

NSPCC visit reference abuse and E-safety
Visiting speaker - E-safety specific

Additional assemblies and speakers periodically through the year as required

Appendix 9 – Online Safety Information and support

There is a wealth of information available to support schools and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Organisation/Resource	What it does/provides
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Be Internet Legends Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and Directors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • free online safety tool for schools is provided alongside questions for the governing board concerning online safety. • Education for a Connected World
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning