Fulbrook Middle School

E- Safety Policy
Computer and Acceptable Use

Issue No.	Author or Reviewer	Date Written or Reviewed	Date Approved by FES/PEAP	Date Approved by FGB	Next Review Date
	S Thomas	October 2015	October 2015	October 2015	October 2016
	S Clancy	Sept. 2016	Sept 2016	Oct 2016	Sept 2017
	S Thomas	March 2018			
	S Thomas	November 2019	14 November 2019	18 December 2019	November 2021

Development / Monitoring / Review of this Policy

- *E-Safety Co-Ordinator / Deputy Safeguarding lead S Thomas*
  Deputy Head Teacher/Designated Safeguarding Lead – J Wall
- *Technical staff – S Howe / G Peck(Partnership Education)*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *PEA&P Committee on:*	*14 November 2019*
The implementation of this e-safety policy will be monitored by the:	*E-Safety Coordinator* *PEA&P Committee, Senior Leadership Team,*
Monitoring will take place at regular intervals:	*Termly*
The PEA&P Committee (and the FGB as appropriate) will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*At least yearly/at FGB via the Head's Report to Governors as necessary*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*Yearly*

Scope of the Policy

This policy applies to all members of Fulbrook Middle School community (including staff, pupils, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of Fulbrook Middle School ICT systems, both in and out of Fulbrook Middle 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 Fulbrook Middle 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 outside of the Fulbrook Middle School, but is linked to membership of Fulbrook Middle School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Fulbrook Middle 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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the PEA&P Committee receiving regular information about e-safety incidents and monitoring reports.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and at least one other member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher 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 Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator:

- 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 school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments integris.
- meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering

- attends relevant meeting with Governors
- reports regularly to the Senior Leadership Team

Network Manager / Technical staff:

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

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that Fulbrook Middle School meets required e-safety technical guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with 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 / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety co-ordianator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in Fulbrook Middle School policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Fulbrook Middle School e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers 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 activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned pupils 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*

Child Protection / Safeguarding Designated Officer

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

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

Pupils:

- are responsible for using Fulbrook Middle School digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand 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 / academy's* E-Safety Policy covers their actions out of school, if related to their membership of the school

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. Fulbrook Middle School will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support *Fulbrook Middle School* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices in Fulbrook Middle School (where this is allowed)

Community Users

Community Users who access school systems / website as part of the wider *Fulbrook Middle School* provision will be expected to sign a Community User AUA before being provided with access to school systems.

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

- A planned e-safety curriculum should be provided as part of Computing lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of assemblies and phse activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students 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 Technical Staff (ST) 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.

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats.

It is therefore important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching could be built into existing lessons across the curriculum, covered within specific online safety lessons and/or school wide approaches.

Teaching must always be age and developmentally appropriate.

Underpinning knowledge and behaviours include:
How to evaluate what they see online - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

Schools can help pupils consider questions including:
is this website/URL/email fake? How can I tell?
what does this cookie do and what information am I sharing?
is this person who they say they are?
why does someone want me to see this?
why does someone want me to send this?
why would someone want me to believe this?
why does this person want my personal information?
is this too good to be true?

is this fact or opinion?

How to recognise techniques used for persuasion.
This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

Schools can help pupils to recognise:
online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation), techniques that companies use to persuade people to buy something,

ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and criminal activities such as grooming.

Online behaviour
This will enable pupils to understand what acceptable and unacceptable online behaviour look like. Schools should teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Schools should also teach pupils to recognise unacceptable behaviour in others.

Schools can help pupils to recognise acceptable and unacceptable behaviour by:
looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do, looking at how online emotions can be intensified resulting in mob mentality,1 teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

How to identify online risks This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

Schools can help pupils to identify and manage risk by:
discussing the ways in which someone may put themselves at risk online, discussing when risk taking can be positive and negative, online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example, 1 Mob mentality describes how people can be influenced by their peers to adopt certain behaviors on a largely emotional, rather than rational, basis discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

How and when to seek support.
This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

Education – parents / carers

Many parents and carers have only 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website,
- Parents / Carers evenings / sessions
- High profile events / campaigns

Education – The Wider Community

Fulbrook Middle School will provide opportunities for local community groups / members of the community to gain from the school's / academy's e-safety knowledge and experience. This may be offered through the following:

- Providing Adult learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- Fulbrook Middle School website will provide e-safety information for the wider community

Education & Training – Staff / Volunteers

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 formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly

It is expected that some staff will identify e-safety as a training need within the performance management/Appraisal process.

- 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 Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any form of child protection. This may be offered in a number of ways:

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

Technical – infrastructure / equipment, filtering and monitoring

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

- Technical systems will be managed in ways that ensure that Fulbrook Middle School meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Fulbrook Middle School technical systems and devices.
- All users will be provided with a username and secure password by ST (Fulbrook Middle School) or SH or GP (Partnership Education) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly.
- The "master / administrator" passwords for Fulbrook Middle School ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- ST is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

- Internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering.
- The school has provided enhanced / differentiated user-level filtering
- Fulbrook Middle School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place (email ST/or partnership education) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social

networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- 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.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

See:
Fulbrook Data Protection Policy 2018
Fulbrook Data Retention Policy 2018

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x				x			
Use of mobile phones in lessons		x						x
Use of mobile phones in social time		x						x
Taking photos on mobile phones / cameras		x						x
Use of other mobile devices e.g. tablets, gaming devices	x							x
Use of personal email addresses in school, or on school network	x							x
Use of school email for personal emails	x				x			
Use of messaging apps	x							x
Use of social media	x							x
Use of blogs	x							x

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

- The official *Fulbrook Middle School* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only Fulbrook Middle School email service to communicate with others when in school, or on Fulbrook Middle School systems (e.g. by remote access).
- Users must immediately report, to the nominated person (ST) – in accordance with Fulbrook Middle Schools policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents / carers (email etc.) must be professional in tone and content. These communications may only take place on official (monitored) Fulbrook Middle School systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will be provided with individual Fulbrook Middle School email addresses for educational use.
- Pupils will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on Fulbrook Middle Schools website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Fulbrook Middle School liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer (Headteacher) to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

The school 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. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	

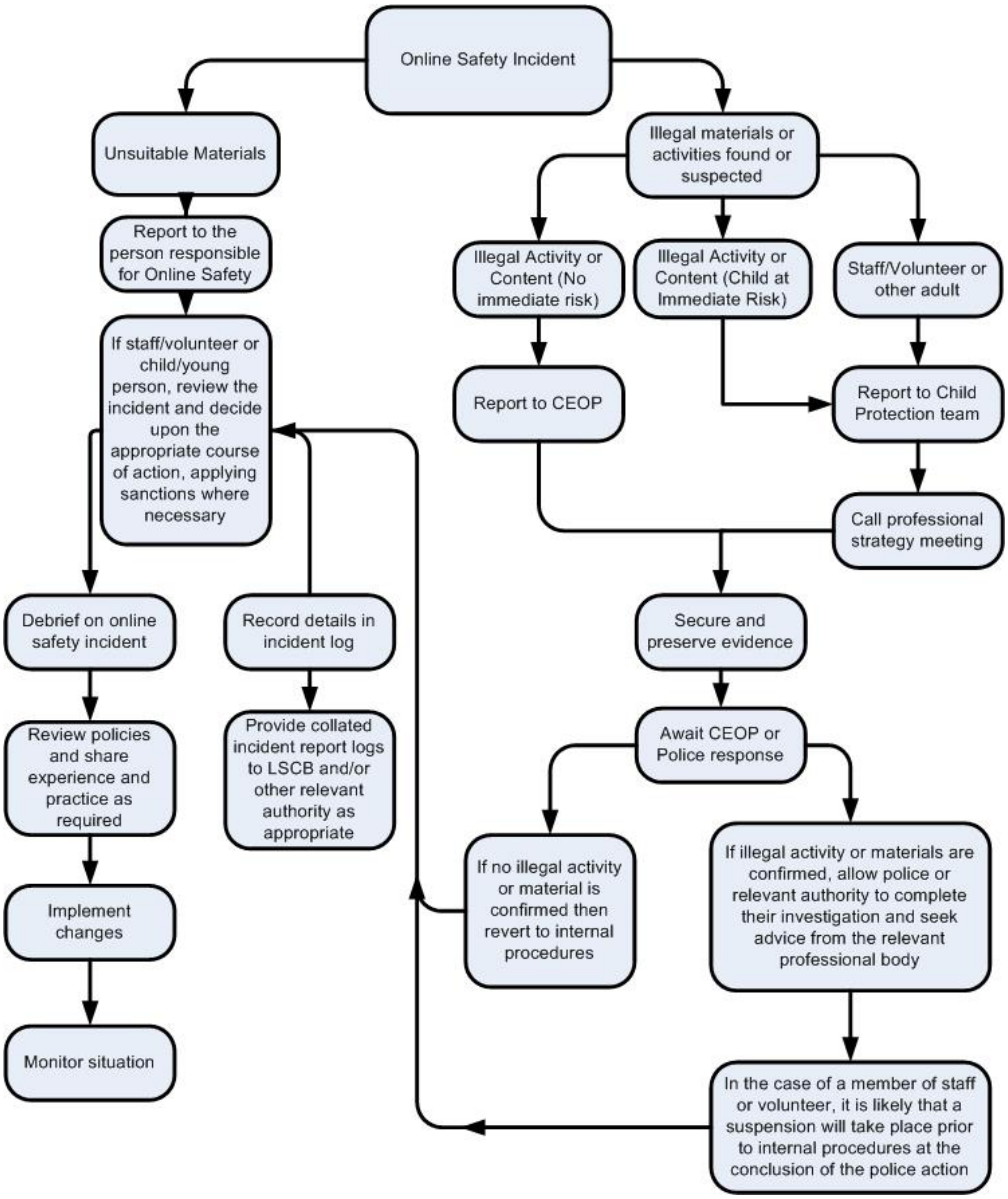
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Fulbrook Middle School				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non educational)				X	
On-line gambling			X		
On-line shopping / commerce		X			
File sharing		X			
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting e.g. YouTube		x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). Incidents should also be logged on integris and MyConcern as appropriate.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies; they understand and follow Fulbrook Middle Schools policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures

- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

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

It is important that all of the above steps are taken as they will provide an evidence trail for Fulbrook Middle School (and possibly the police) and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Fulbrook Middle School Actions & Sanctions

It is more likely that Fulbrook Middle 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:

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal		X	X	X					
Unauthorised use of non-educational sites during lessons								X	
Unauthorised use of mobile phone / digital camera / other mobile device		x				x		X	X
Unauthorised use of social media / messaging apps / personal email					X	X	x	X	X
Unauthorised downloading or uploading of files					X		x	X	X
Allowing others to access Fulbrook Middle School network by sharing username and passwords	x					X	x	X	
Attempting to access or accessing Fulbrook Middle School network, using another student's / pupil's account	x	x			X		x	X	
Attempting to access or accessing Fulbrook Middle School network, using the account of a member of staff		x	x		X	X	x	X	X
Corrupting or destroying the data of other users		x	x		X	X	x	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x			X	X		X	
Continued infringements of the above, following previous warnings or sanctions		x	x	X	X	X	x		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x		X	X	x	X	X
Using proxy sites or other means to subvert the school's filtering system		X				X	x	X	
Accidentally accessing offensive or pornographic material and failing to report the incident					X	X		X	
Deliberately accessing or trying to access offensive or pornographic material			x		x	x	x	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x		x	X		x	

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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).		X	X	X				x
Inappropriate personal use of the internet / social media / personal email		X	x		X	X		
Unauthorised downloading or uploading of files		X				X		
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		X			X	X		x
Careless use of personal data e.g. holding or transferring data in an insecure manner		x			x	X		X
Deliberate actions to breach data protection or network security rules		X	x		X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x	x	X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	x			X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		x	x	X				
Actions which could compromise the staff member's professional standing		x	x			X		
Actions which could bring Fulbrook Middle School into disrepute or breach the integrity of the ethos of Fulbrook Middle School		X	x			X		X
Using proxy sites or other means to subvert the school's filtering system		x	X		X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	x		X	X		x
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions			x			x	x	x