Crofty Multi Academy Trust

Online Safeguarding Policy

Date of Drafting: May 2020

Adopted Date: June 2020

Review Date: June 2022

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safeguarding incidents covered by this policy, which may take place outside of the *school*, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

The following section outlines the Online Safeguarding roles and responsibilities of individuals and groups within the trust.

Trust Online Safeguarding Group

The Online Safeguarding Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safeguarding and the monitoring the Online Safeguarding Policy including the impact of initiatives. Depending on the size or structure of the school, this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body / Board of Trustees.

Members of the Online Safeguarding Group will assist the Online Safeguarding Co-ordinator with:

- Regular review of the current Online Safeguarding provision using the 360 degree safe tool
- Provide strategic direction in regarding to Online Safeguarding
- Ensuring that Online Safeguarding is satisfactorily covered within the curriculum
- Monitoring network / internet / incident logs
- Consulting all stakeholders including parents and students about the Online Safeguarding provision.

Board of Trustees

The Board of Trustees are responsible for the approval of the Online Safeguarding Policy. The Trust Online Safeguarding team is responsible for reviewing the effectiveness of the policy. This will be carried out by receiving regular information about Online Safeguarding incidents and monitoring reports.

Headteachers and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including Online Safeguarding) of members of the school community, though the day to day responsibility for Online Safeguarding will be delegated to the Online Safeguarding Coordinator.
- The Headteacher and (at least) one other member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safeguarding allegation being made against a member of staff. (see flow chart on dealing with Online Safeguarding incidents – included in a later section – "Responding to incidents of misuse" and relevant Trust disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safeguarding roles and to train other colleagues, as relevant.
- The Headteacher and 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 Online Safeguarding 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 Online Safeguarding Coordinator.

Online Safeguarding Coordinator

Each school will have an Online Safeguarding Coordinator. In most cases, this will form part of the role of the Computing Coordinator. Their responsibilities include:

- taking day to day responsibility for Online Safeguarding issues and has a leading role in establishing and reviewing the school Online Safeguarding policies/documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safeguarding incident taking place.
- providing training and advice for staff
- liaising with the Trust Online Safeguarding team
- liaising with school technical staff
- receiving reports of Online Safeguarding incidents and creates a log of incidents to inform future Online Safeguarding developments,

Network Manager / IT Strategy Manager

Those with technical responsibilities are responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- 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 Online Safeguarding technical information in order to effectively carry out their Online Safeguarding role and to inform and update others as relevant
- that the use of the trust's IT systems is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Senior Leaders for investigation / action / sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of Online Safeguarding matters and of the current school Online Safeguarding Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher / Senior Leader / Online Safeguarding 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
- Online Safeguarding issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the academies Online Safeguarding Policy 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

Designated Safeguarding Lead

Should be trained in Online Safeguarding 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
- online-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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 online-bullying.
- should understand the importance of adopting good Online Safeguarding practice when using digital technologies out of school and realise that the school's Online Safeguarding 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national / local Online Safeguarding campaigns/literature. Parents and carers will be encouraged to support the school in promoting good Online Safeguarding 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

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 Online Safeguarding / digital literacy is therefore an essential part of the school's Online Safeguarding provision. Children and young people need

the help and support of the school to recognise and avoid Online Safeguarding risks and build their resilience.

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

- A planned Online Safeguarding curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key Online Safeguarding messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral 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 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.

Education – Parents / Carers

Many parents and carers have only a limited understanding of Online Safeguarding risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online 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, Web site,
- Parents / Carers evenings / Sessions
- High profile events/campaigns e.g. Safer Internet Day

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's Online Safeguarding knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and Online Safeguarding
- Online Safeguarding messages targeted towards the whole family
- The school website will provide Online Safeguarding information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safeguarding provision.

Education & Training – Staff/Volunteers

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

- A planned programme of formal Online Safeguarding training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safeguarding training needs of all staff will be carried out regularly.
- All new staff should receive Online Safeguarding training as part of their induction programme, ensuring that they fully understand the Online Safeguarding Policy and Acceptable Use Agreements.
- It is expected that some staff will identify Online Safeguarding as a training need within the performance management process.
- The Online Safeguarding Coordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safeguarding Policy and its updates will be presented to and discussed by staff in staff / team meetings / training sessions.
- The Online Safeguarding Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors / Board of Trustees

Governors / Board of Trustees should take part in Online Safeguarding training / awareness sessions, with particular importance for those who are members of any group involved in technology / Online Safeguarding / health and safety.

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 Online Safeguarding responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school technical systems and devices.
- Users (at KS2 and above) may be provided with a username and secure password by the Trust IT staff / ICT support provider *who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password*.* Academies may choose to use group or class log-ons and passwords (preferably for KS1 and below).
- IT Strategy Manager 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 (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 changes.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering.
- An appropriate system is in place 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 devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be school owned / provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safeguarding education programme.

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 online-bullying 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
- 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 in 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. 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.
- Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO). The school may also wish to appoint a Data Manager and systems controllers to support the DPO.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.

- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care 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" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Ensure that encrypted email is used when sending personal information out of the organisation.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

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 (PTO):

Communication Technologies	Staff & other adults			Pupils				
	ved	d at nes	for taff	ved	owed	d at nes	vith ion	ved
Mobile phones may be brought to the 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	

Further clarification regarding the use of Mobiles Phones may be found in the school's Mobile Phone Policy.

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. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report, to the nominated person – in accordance with the school 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 must be professional in tone and content made through the school/secretary email address. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class / group email addresses may be used at KS1. Pupils at KS2 and above may be provided with individual school email addresses for educational use.
- Pupils should be taught about Online Safeguarding 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.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools / academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority / MAT 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:

- Ensuring that personal information is not published
- Training is provided including: 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 or local authority / MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established they should be regularly checked by the Online Safeguarding Team to ensure compliance with the Social Media, Data Protection, Communications, Digital Images and Video policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would

be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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 / or outside the 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,	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	
	Promotion of extremism or terrorism				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	

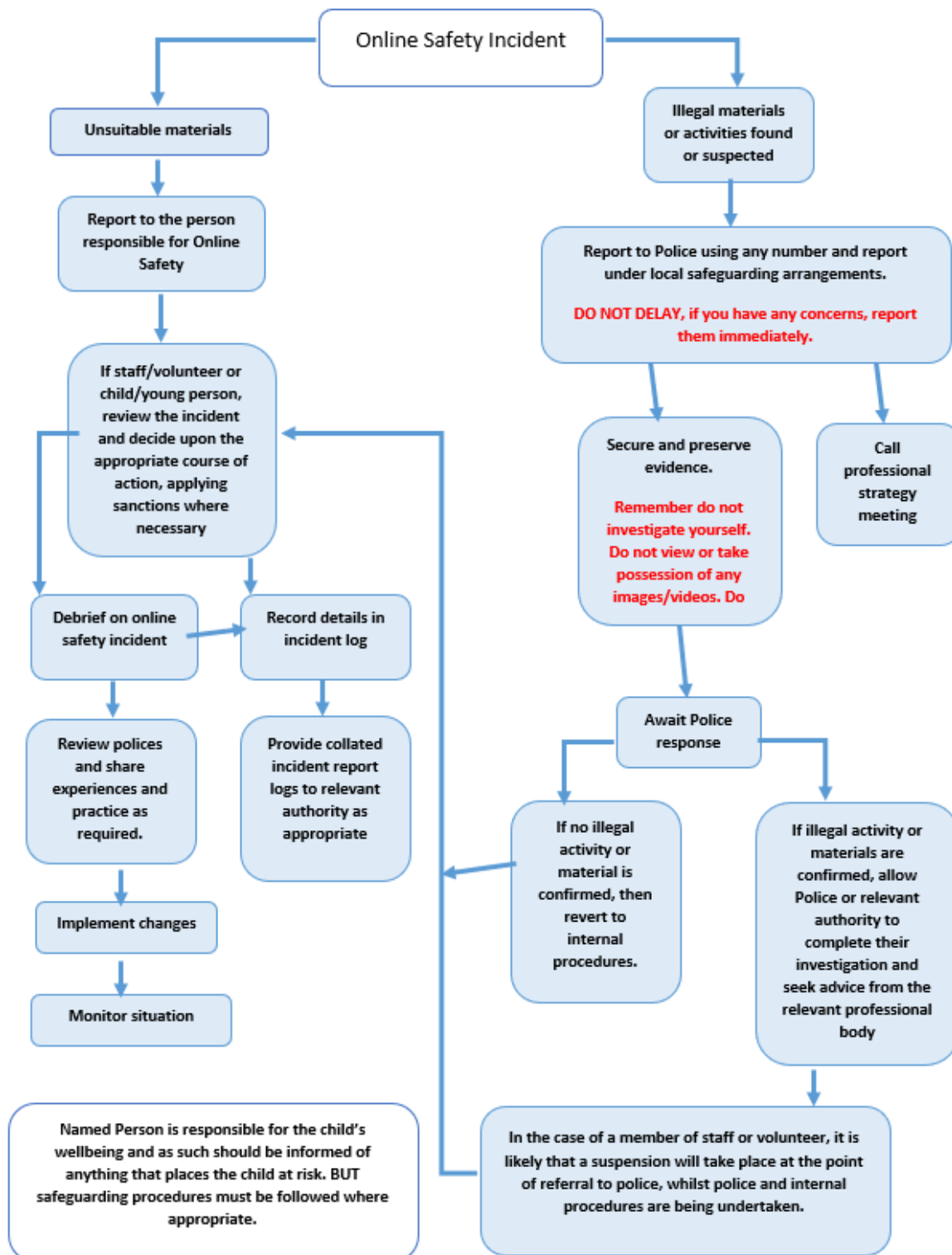|					
proposals or comments that contain or relate to:					
Activities that might be classed as cyber-crime under the Computer Misuse Act: - Gaining unauthorised access to school networks, data and files, through the use of computers/devices - Creating or propagating computer viruses or other harmful files - Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) - Disable/Impair/Disrupt network functionality through the use of computers/devices - Using penetration testing equipment (without relevant permission)					X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				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.

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 for responding to Online Safeguarding incidents and report immediately to the police.

Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

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

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

Concerns around pupil safeguarding must result on an immediate call to LADO : 01872 326536/324954

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated it will needed to be judged whether this concern has substance or not. A conversation with LADO will help make a final decision regarding action to be taken. If it does then appropriate action will be required and could include the following:
    o Internal response or discipline procedures
    o Involvement by Local Authority/School Group or national/local organisation (as relevant).
    o 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/LADO immediately. Other instances to report to the police would include:
    o incidents of 'grooming' behaviour
    o the sending of obscene materials to a child
    o adult material which potentially breaches the Obscene Publications Act
    o criminally racist material
    o promotion of terrorism or extremism
    o offences under the Computer Misuse Act (see User Actions chart above)
    o other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School actions & sanctions

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/safeguarding procedures as follows (PTO):

Actions/Sanctions

	Refer to class teacher/tutor	Refer to Headteacher	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 eg detention/exclusion
Pupils Incidents								
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X			X			
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X		X	X			
Unauthorised downloading or uploading of files	X			X			X	
Allowing others to access school network by sharing username and passwords	X			X			X	
Attempting to access or accessing the school network, using another student's/pupil's account	X			X			X	
Attempting to access or accessing the school network, using the account of a member of staff	X			X			X	

Corrupting or destroying the data of other users	X	X		X	X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X			
Continued infringements of the above, following previous warnings or sanctions	X	X			X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X			
Using proxy sites or other means to subvert the school'sfiltering system	X			X			X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X	X			X
Deliberately accessing or trying to access offensive or pornographic material	X		X				X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act								

Actions/Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Police /LADO	Refer to Technical Support Staff for action re filtering etc.	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		
Inappropriate personal use of the internet/social media/personal email	X			X	X
Unauthorised downloading or uploading of files	X	X		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
Careless use of personal data e.g. holding or transferring data in an insecure manner	X			X	X
Deliberate actions to breach data protection or network security rules		X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils		X			X

Actions which could compromise the staff member's professional standing		X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X
Using proxy sites or other means to subvert the school'sfiltering system		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
Breaching copyright or licensing regulations	X				**X**
Continued infringements of the above, following previous warnings or sanctions		X			X