Hodgson Academy

*****

On Line Safeguarding Policy

Contents

Development / Monitoring / Review of this Policy

This online safeguarding policy has been developed by a working group / committee made up of:

- *Headteacher / Principal / Senior Leaders*
- *Online safeguarding officer*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*

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

Schedule for Development / Monitoring / Review

This online safeguarding policy was approved by the Governing Body *on:*	2nd October 2018
The implementation of this online safeguarding policy will be monitored by the:	*Online safeguarding Officer* *Online safeguarding Committee* *Senior Leadership Team*
The Governing Body will receive a report on the implementation of the policy generated by the monitoring group (which will include anonymous details of online safeguarding incidents) at regular intervals:	*Every governors meeting*
The Online safeguarding 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 online safeguarding or incidents that have taken place. The next anticipated review date will be:	2nd October 2019
Should serious online safeguarding incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

Scope of the Policy

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

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

The academy 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 *academy*:

Governors:

Governors are responsible for the approval of the online safeguarding policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safeguarding incidents and monitoring reports. A member of the Governing Body has taken on the role of *Online safeguarding Governor*. The role of the Online safeguarding Governor will include:

- regular meetings with the Online safeguarding Officer
- ensuring regular monitoring of online safeguarding incident and monitoring of filtering / change control logs takes place
- ensures that reports are made to the full governing body

Principal and Senior Leaders:

- The *Principal* 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 safety officer.
- The Principal and another member of the Senior Leadership Team / Senior Management 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”.
- The Principal Senior Leaders are responsible for ensuring that the Online safeguarding Officer 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 Principal / 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 Co-ordinator / Officer.

Online safeguarding Coordinator / Officer:

- leads the online safeguarding committee
- takes day to day responsibility for online safeguarding issues and has a leading role in establishing and reviewing the school online safeguarding policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safeguarding incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safeguarding incidents and creates a log of incidents to inform future online safeguarding developments
- meets regularly with Online safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant committee of Governors.
- reports regularly to Senior Leadership Team.

- 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
    - cyber-bullying

Network Manager:

The Network Manager is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the academy meets required online safeguarding technical requirements
- 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 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 network / internet / Virtual Learning Environment / remote access / email is regularly monitored by appropriate software in order that any misuse / attempted misuse can be reported to the Principal / Senior Leader; Online safeguarding Officer for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy 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 *academy* online safeguarding 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 *Principal / Senior Leader ; Online safeguarding Officer* for investigation / action / sanction
- all digital communications with students / 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

- students understand and follow the online safeguarding and acceptable use policies
- students 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

Online safeguarding group

The Online safeguarding Group provides a consultative group that has wide representation from the *academy* community, with responsibility for issues regarding online safeguarding and the monitoring the online safeguarding policy including the impact of initiatives. The group will also be responsible for regular reporting to the *Governing Body*

Members of the *Online safeguarding Group* (or other relevant group) will assist the *Online safeguarding Officer (or other relevant person, as above)* with:

- the production / review / monitoring of the school online safeguarding policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the online safeguarding curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safeguarding provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students / pupils:

- are responsible for using the *academy* digital technology systems in accordance with the Student 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 online safeguarding practice when using digital technologies out of school and realise that the *academy'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 *academy* will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online safeguarding campaigns / literature. Parents and carers will be encouraged to support the *academy* 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 records
- their children's personal devices in the school / academy (where this is allowed)

Community Users

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

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* in online safeguarding 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 progress tutor activities
- Students 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.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the student 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 students / 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 students / 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated 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.

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 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:

- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

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 school online safeguarding policy and Acceptable Use Agreements.
- The Online safeguarding Officer (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 / INSET days.
- The Online safeguarding Officer (or other nominated person) will provide advice / guidance / training to individuals as required

Training – Governors

Governors should take part in online safeguarding training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / online safeguarding / health and safety / 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 (eg SWGfL).
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The academy 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 / Academy technical systems will be managed in ways that ensure that the school / academy 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 school / academy technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager 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 every term.*
- The "master / administrator" passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher / Principal* or other nominated senior leader and kept in a secure place (e.g. school safe).
- The Network 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
- The academy has provided enhanced / differentiated user-level filtering.
- Academy 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 for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).

- Appropriate security measures are in place 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.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students 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 students 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 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 students / 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students 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.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website this will be collected as part of the data collection exercise at the start of the academic year and will be recorded within the academy's MIS.
    - As part of the data collection exercise parents/carers will have the option to tick if they wish their child's photograph to be published.

Please also refer to the academy's 'Use of Photographic, Digital & Video Images Policy

Data Protection

Please refer to the academy's Data Protection Policy

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			Students				
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	✓				✓			
Use of mobile phones in lessons		✓					✓	
Use of mobile phones in social time	✓							
Taking photos on mobile phones / cameras*		✓					✓	
Use of other mobile devices e.g. tablets, gaming devices	✓					✓		
Use of personal email addresses in school, or on school network	✓				✓			
Use of school email for personal emails	✓			✓				
Use of messaging apps	✓					✓		
Use of social media		✓					✓	
Use of blogs		✓					✓	

**Photographs should be deleted as soon as possible in line with professional working practice. Any photographs that are stored will be done so in line with data protection regulation.*

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

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school / academy 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 students or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school /

academy systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Students 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.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.
- Staff should not send e mails between the period 6.00pm and 7.30am on weekdays and no e-mails should be sent on weekends.
- Language within all communication should be appropriate to a business environment and the tone should be business-like at all times. The school maintains the right to access and check all school email accounts as agreed in the Approved Use Policy.
- If absent a member of staff must follow the procedures within our attendance policy and not communicate the absence via email. The member of staff may choose to send work via email but must check that the work has been received by the appropriate person in school.
- Emails should be checked once during the school day. Therefore it is important not to send emails that require action that day as the recipient may not open the email until the end of the day. Other messages, that require action that day, may be communicated verbally. Please be mindful of staff welfare when setting deadlines. Only on rare occasions for very urgent jobs should staff be asked to complete a task on the same day e.g. setting work for isolated students.

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 any protected characteristic or who defame a third party may render the *academy* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy 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 students, 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 *academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Professional judgment should be used to decide if former students under 18 should be added as 'friends' or 'followers' for any personal social media account. Current students should not be added. Staff should contact their line manager if personal circumstances (e.g. students who are family members) would challenge this position.

The *academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and online safeguarding committee 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:

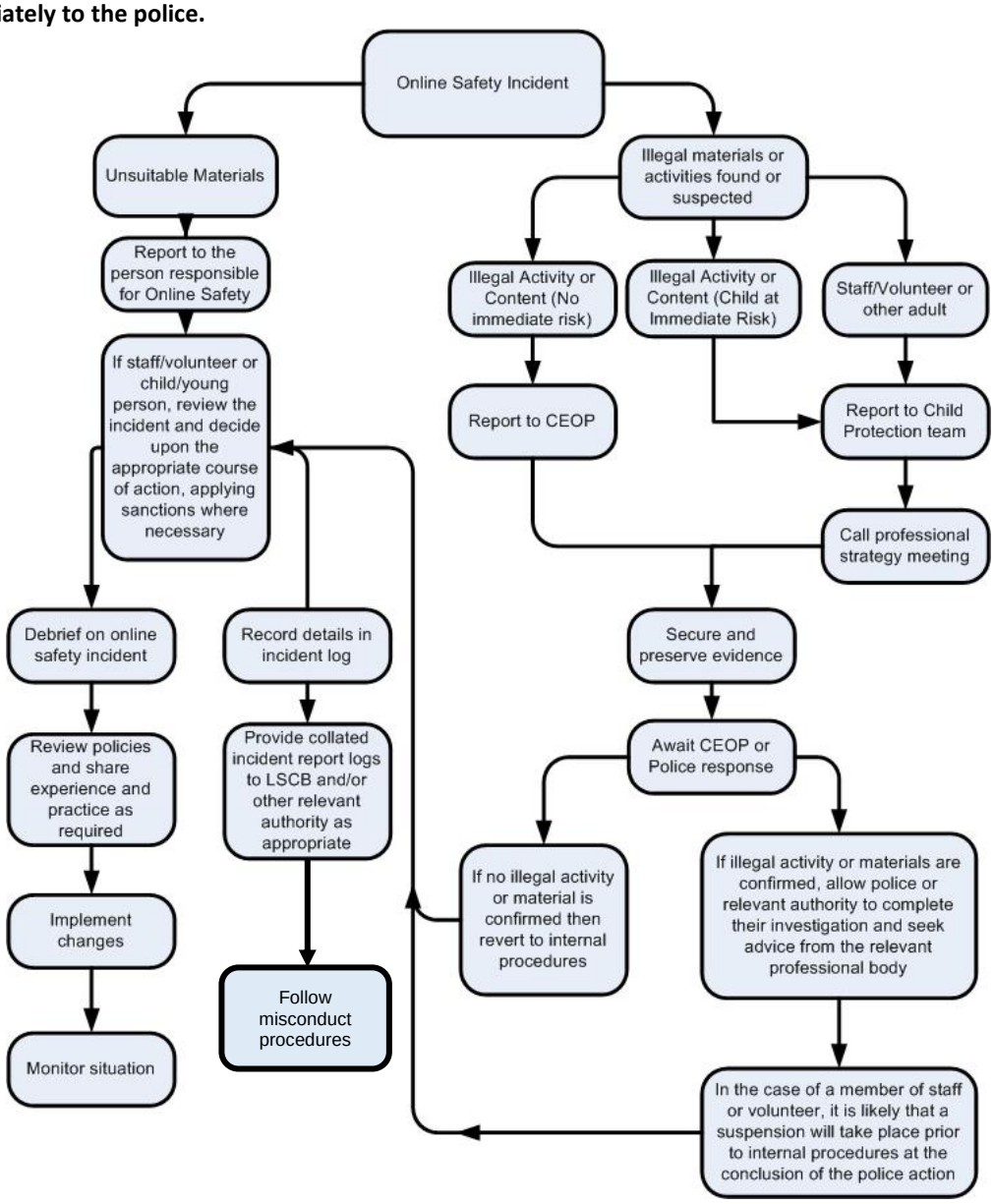
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child 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	X
	threatening behaviour, including promotion of physical violence or mental harm				X	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 school / academy					X	
Infringing copyright					X	X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	X
Creating or propagating computer viruses or other harmful files					X	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). SWGfL BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (http://www.swgfl.org.uk/Staying-Safe/Online safeguarding-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool)

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 safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow academy 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 the *academy* 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.

Academy Actions & Sanctions

It is more likely that the academy 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. Not following this policy could lead to a warning, suspension or disciplinary action. If any individual was suspected of the breaking the law they would be referred to the police.

E-safe

The Academy are registered with e-safe to ensure that any safeguarding incidents that arise from computer use by students is identified and an incident report is sent to the online safeguarding officer, the Principal and the Deputy Principal. The incident depending on its severity can then be referred to the relevant staff members and/or external agencies. In addition to this any use of inappropriate language or searches will also be highlighted so that they may be

dealt with accordingly. All students and staff have been made aware of the installation of e-safe across school and how it works.

Acknowledgements

The policy has been adapted from the policy available from: http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online safeguarding Policy Template and of the 360 degree safe Online safeguarding Self Review Tool:

- Members of the SWGfL Online safeguarding Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids