Appendices

Responsible Computer Use Agreement

A Guide to Using Images Online

Responding to incidents of misuse – flowchart

Incident Reporting Log

Training Log

School Technical Security Policy

Filtering

Social Media Policy

Legislation

Links to other organisations or documents

Glossary of terms

Responsible Computer Use Agreement

When using the computers:

- I will only access the computer system with the login and password that I have been given
- I will not access other people's files unless they are my Computing partner
- I will not bring in memory sticks from home to use on the network

When using the internet:

- I will ask permission before I access it
- I will report any material that makes me feel uncomfortable **immediately** to my teacher
- I understand that the school may check my files and monitor the sites that I visit
- I will not knowingly access social networking sites or chat rooms
- I will **never** give my full name, address, telephone number or agree to meet anyone
- I will not use search engines to find inappropriate material

I understand that:

- Using computers safely can make everyone's learning more enjoyable

General Internet Safety Tips

- Always ask a grown up before you use the internet. They can help you find the best thing to do
- Don't tell strangers where you live, your phone number or where you go to school. Only your friends and family need to know that
- Don't send pictures to people you don't know. You don't want strangers looking at photos of you, your friends or your family
- Tell a grown-up if you feel scared or unhappy about anything. Ask a grown up to help you put the Hector's World Safety Button on your computer. This will mean that you can press it if anything makes you scared or unhappy.
- You can also call 'Childline' on 0800 1111 to talk to someone who can help

www.thinkuknow.co.uk www.ceop.police.uk

Guide to the Use of Images Online

Using Images Safely and Responsibly

We all enjoy and treasure images of our family and friends; family events, holidays and events are moments we all like to capture in photos or on video.

We now have the exciting option of adding our images and videos to our online social networks, such as Facebook, YouTube and many other websites. This means that we can easily share our photos and videos with family and friends.

Whilst this can be very useful to all of us, we must ensure we protect and safeguard all children and staff, including those who do not want to have their images stored online.

What are the risks of posting images online?

- Once posted and shared online any image or video can be copied and will stay online forever.
- Some children are at risk and MUST NOT have their image put online. Not all members of the community will know who they are.
- Some people do not want their images online for personal or religious reasons.
- Some children and staff may have a complex family background which means that sharing their image online can have unforeseen circumstances.

Therefore, at Elston Hall we are happy for parents and carers to take photos and video events for personal use but **insist** that these images are not distributed or put online in any way. This is to protect all members of the school community.

We thank you for your support,

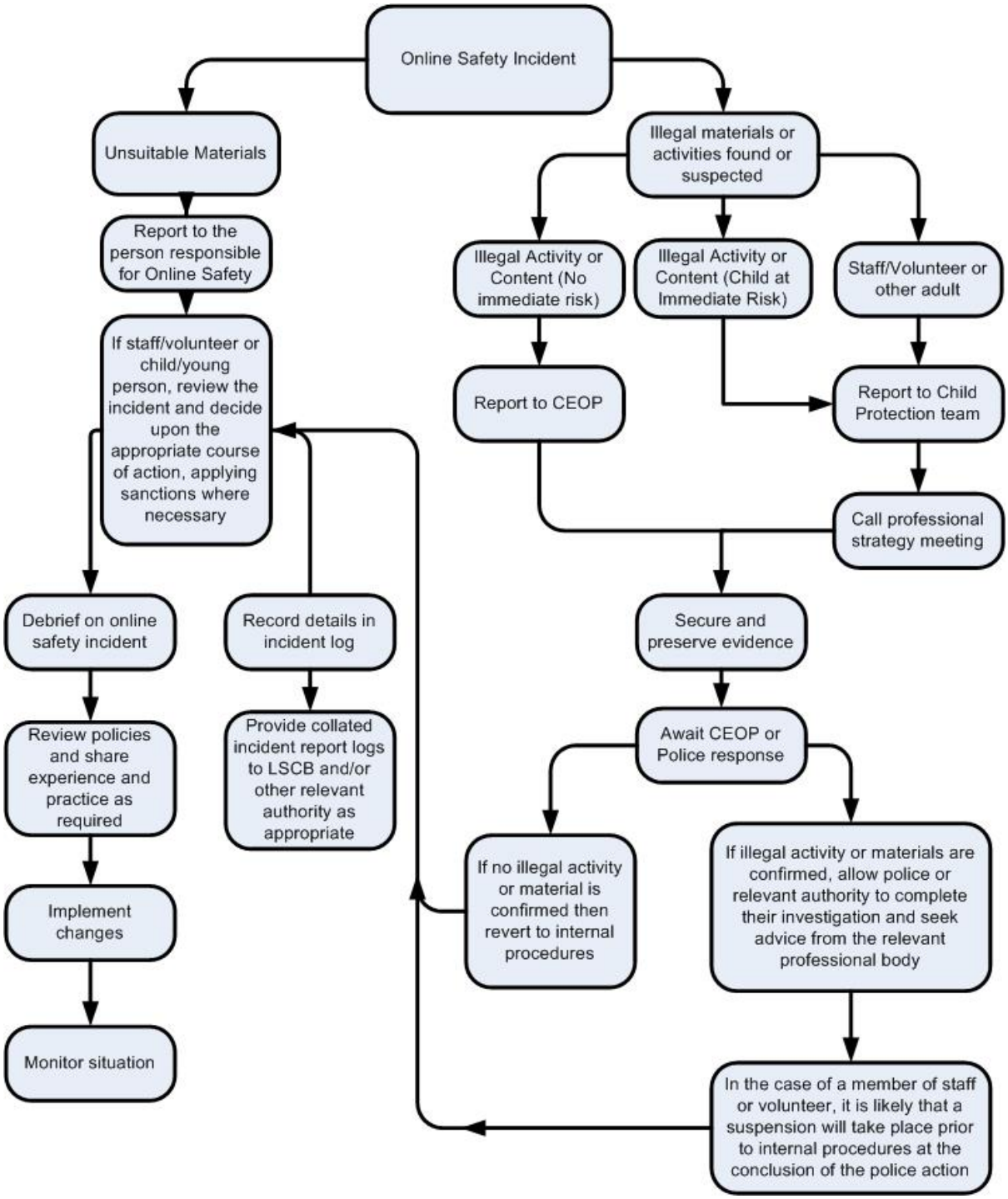
Further Information on the Use of Images and Video:

Get Safe Online: https://www.getsafeonline.org/

Think U Know: https://www.thinkuknow.co.uk/parents/

Our website: https://www.elstonhallmat.co.uk/

Responding to incidents of misuse – flow chart



Incident Log

Academic Year _____

Person involved	*Nature of Incident*	*Date/Time*	*Reported to*	*Action Taken*

Training Log

Group: .....

Relevant training the last 12 months	*Identified Training Need*	*To be met by*	*Cost*	*Review Date*

Elston Hall MAT Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

If the *school / academy* has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the *school / academy* itself (as suggested below). It is also important that the managed service provider is fully aware of the *school / academy* Online Safety Policy / Acceptable Use Agreements). The *school / academy* should also check their Local Authority / Academy Group / other relevant body policies / guidance on these technical issues.

Responsibilities

The management of technical security will be the responsibility of (insert title) (schools will probably choose the Network Manager / Technical Staff / Head of Computing or other relevant responsible person)

Technical Security

Policy statements

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 receive guidance and training and will be effective in carrying out their responsibilities: (schools will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy:)

- **School / Academy technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements** (these may be outlined in Local Authority / Academy Group / other relevant body technical / online safety policy and guidance)
- **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**
- **Appropriate security measures are in place** (schools may wish to provide more detail) **to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff** (schools may wish to provide more detail).
- **All users will have clearly defined access rights to school / academy technical systems.** *Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).*
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. *(See Password section below).*
- (Insert name or role) 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- *Mobile device security and management procedures are in place* (for school / academy provided devices and / or where mobile devices are allowed access to school systems). (Schools / academies may wish to add details of the mobile device security procedures that are in use).
- School / 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. (schools / academies may wish to add details of the monitoring programmes that are used).
- *Remote management tools are used by staff to control workstations and view users activity*
- *An appropriate system is in place* (to be described) *for users to report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed).*
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.

- *An agreed policy is in place* (to be described) *regarding the downloading of executable files and the installation of programmes on school devices by users*
- *An agreed policy is in place* (to be described) *regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place* (to be described) *regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.* (see School Personal Data Policy Template in the appendix for further detail)
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured*. (see School Personal Data Policy Template in the appendix for further detail)

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE). Where sensitive data is in use – particularly when accessed on laptops / tablets – schools may wish to use more secure forms of authentication e.g. two factor authentication such as the use of hardware tokens and if so should add a relevant section in the policy. Where this is adopted, the policy should state clearly that such items as hardware tokens must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- **All school / academy networks and systems will be protected by secure passwords that are regularly changed**
- **The "master / administrator" passwords for the school / academy systems, used by the technical staff must also be available to the *Headteacher / Principal* or other nominated senior leader and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts**. (A school / academy should never allow one user to have sole administrator access)
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- *Passwords for new users, and replacement passwords for existing users will be allocated by xxxxx (insert title) (schools may wish to have someone other than the school's technical staff*

carrying out this role eg an administrator who is easily accessible to users). Any changes carried out must be notified to the manager of the password security policy (above). Or:

- *Passwords for new users and replacement passwords for existing users will be issued through an automated process* (to be described)
- *Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below* (The level of security required may vary for staff and student / pupil accounts and the sensitive nature of any data accessed through that account)
- *Where passwords are set / changed manually requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user* (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

Staff Passwords

- **All staff users will be provided with a username and password** by (insert name or title / automated process) who / which will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- *must not include proper names or any other personal information about the user that might be known by others*
- *the account should be "locked out" following six successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school*
- should be changed at least every 60 to 90 days (Some organisations require changes each month / / 6 weeks. The frequency should depend on the nature of the account and how sensitive / damaging loss of data would be. It would be reasonable to require staff password changes more frequently that student / pupil password changes)
- should not re-used for 6 months and be significantly different from previous passwords created by the same user. *The last four passwords cannot be re-used*.

Student / Pupil Passwords

Primary schools will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class log-ins for KS1 (though increasingly children are using their own passwords to access programmes). *Schools / academies* need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by pupils in this way should always be supervised and members of staff

should never use a class log on for their own network / internet access. Schools / Academies should also consider the implications of using whole class log-ons when providing access to learning environments and applications, which may be used outside school.

- **All users** (at KS2 and above) **will be provided with a username and password** by (insert name or title / automated routine) who / which will keep an up to date record of users and their usernames.
- *Users will be required to change their password every (insert period).*
- Students / pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children. *(to be described)*

Schools / academies may wish to add to this list for all or some students / pupils any of the relevant policy statements from the staff section above.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ins are being used.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons (the school / academy should describe how this will take place)
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (insert title) will ensure that full records (manual or automated) are kept of:

- User Ids and requests for password changes
- *User log-ins*
- *Security incidents related to this policy*

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot,

however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools / academies. Where available, schools / academies should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

Schools / academies need to consider carefully the issues raised and decide:

- Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation
- Whether to introduce differentiated filtering for different groups / ages of users
- Whether to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used

Responsibilities

The responsibility for the management of the school's filtering policy will be held by (insert title). They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must (schools should choose their relevant responses):

- **be logged in change control logs**
- **be reported to a second responsible person** (insert title):
- *either… be reported to and authorised by a second responsible person prior to changes being made* (recommended)
- *or… be reported to a second responsible person* (insert title) *every X weeks / months in the form of an audit of the change control logs*
- *be reported to the Online Safety Group every X weeks / months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *Either - The school / academy maintains and supports the managed filtering service provided by the Internet Service Provider* (or other filtering service provider)
- *Or – The school / academy manages its own filtering service* (n.b. If a school / academy decides to remove the external filtering and replace it with another internal filtering system, this should be clearly explained in the policy and evidence provided that the Headteacher / Principal would be able to show, in the event of any legal issue that the school was able to meet its statutory requirements to ensure the safety of staff / students / pupils)
- *The school has provided enhanced / differentiated user-level filtering through the use of the* (insert name) *filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher / Principal (or other nominated senior leader).*
- *Mobile devices that access the school / academy internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff* (insert name or title) (nb an additional person should be nominated – to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). *If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.*

Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (amend as relevant)

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc. (amend as relevant)

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering (whether this is carried out in school or by an external filtering provider)
- the grounds on which they may be allowed or denied (schools may choose to allow access to some sites eg social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records / audit of logs)
- any audit / reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make school level changes (as above).

Monitoring

Some schools / academies supplement their filtering systems with additional monitoring systems. If this is the case, schools / academies should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:* (details should be inserted if the school / academy so wishes).

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (schools should amend as relevant)

- the second responsible person (insert title)
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

Further Guidance

Schools / academies may wish to seek further guidance. The following is recommended:

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*

In response UKSIC produced guidance on – information on "Appropriate Filtering"

NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/

Somerset Guidance for schools – this checklist is particularly useful where a school / academy uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **SLT**
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for Social Media accounts
    - Approve account creation
- **Administrator / Moderator**
    - Create the account following SLT approval
    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - *The school permits reasonable and appropriate access to private social media sites.*
- **Pupil/Students**
    - **Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.**
    - The school's education programme should enable the pupils/students to be safe and responsible users of social media.
    - Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
    - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
    - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post

- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently

making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social

workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

Somerset - Questions for Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation

Connectsafely Parents Guide to Facebook

Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom – Children & Parents – media use and attitudes report - 2015

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)

SWGfL South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK Think U Know – educational online safety programmes for schools, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.