Marwood School Online Safety Policy March 2022

Contents

Marwood School Online Safety Policy March 2022 0
Contents 1
Introduction 2
Development/Monitoring/Review of this Policy 5
Roles and Responsibilities 6
Policy Statements 8
Communications 15
Dealing with unsuitable/inappropriate activities 18
Responding to incidents of misuse 20
Illegal Incidents 21
Other Incidents 22
School/academy actions & sanctions 22
Appendix 26
Responding to incidents of misuse – flow chart 27
Record of reviewing devices/internet sites (responding to incidents of misuse) 28
Reporting Log 29
Mobile Technologies Policy Template (inc. BYOD/BYOT) 29
Social Media Policy Template 32
Glossary of Terms 40

Introduction

SWGfL/UK Safer Internet Centre

The South West Grid for Learning Trust is an educational trust with an international reputation for supporting schools with online safety.

SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. The Safer Internet Centre is, for example, responsible for the organisation of Safer Internet Day each February. More information about UKSIC services and resources can be found on the website: www.saferinternet.org.uk. SWGfL is a founding member of UKCIS (UK Council for Internet Safety). It has contributed to conferences across the world and has worked with government and other agencies in many countries. More information about its wide-ranging online safety services for schools can be found on the SWGfL website – swgfl.org.uk

360 degree safe Online Safety Self Review Tool

360 degree safe is an online, interactive self review tool which allows schools/academies to review their online safety policy and practice. It is available, free of charge, to all schools/academies - with over 10,000 registrations, since its introduction in 2009. You can register at 360safe.org.uk. There are also specific versions of the tool available for Scotland – www.360safescotland.org.uk and for Wales. Schools in Wales should access 360Cymru from Hwb.

Schools/academies choose one of 5 level statements in each of the 21 aspects. The tool provides an "improvement action" describing how the school/academy might move from that level to the next. Users can immediately compare their levels to the average levels of all the schools/academies using the tool and to the Online Safety Mark benchmark levels. There is a range of reports that they can use internally or with consultants.

The tool suggests possible sources of evidence, provides additional resources/good practice guidance and collates the school's action plan for improvement. Sections of these policy templates can also be found in the links/resources sections in 360 degree safe.

Schools that reach required benchmark levels can apply for assessment for the Online Safety Mark, involving a half day visit from an accredited assessor who validates the school's self-review. More information about the Online Safety Mark can be found in the Accreditation section of the 360 tool.

Online Safety BOOST packages bring you extra empowerment and support to deal with your online safety challenges, official or otherwise. It comprises a toolkit of apps, services, tools and resources that all go to save time, equip your school to be more sensitive to, and better manage, online safety situations and issues. This document will reference specific aspects of BOOST to illustrate how it integrates with policy. For further information on BOOST, or to subscribe, please visit https://boost.swgfl.org.uk/

Online Data Protection Self-Review Tool

360data is a unique self-review tool designed to help organisations test and improve their data protection policies and practices. Built on the same approach as the award-winning 360 Degree Safe, this tool will help your organisation understand what systems are currently in place and how to improve these.

During your review, you will be able to generate reports with a list of improvement actions to help you move forward with your organisation's data security. All the resources required to enact those recommendations is included in the tool.

The Online Safety Template Policies

These school/academy Online Safety Template Policies are intended to help school/academy leaders produce a suitable online safety policy document which will consider all current and relevant issues, in a whole school/academy context, linking with other relevant policies, such as the child protection/safeguarding, behaviour and anti-bullying policies.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools/academies are bound. Schools/academies must, through their Online Safety Policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school/academy. The policy will also form part of the school's/academy's protection from legal challenge, relating to the use of digital technologies.

In England, schools/academies are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. From 2015, additional duties under the Counter Terrorism and Securities Act 2015 require schools/academies to ensure that children are safe from terrorist and extremist material on the internet. Revised "Keeping Children Safe in Education" guidance obliges schools and colleges in England 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."

These template policies suggest policy statements which, in the view of SWGfL, would be essential in any school/academy Online Safety Policy, based on good practice. In addition there are a range of alternative statements that schools/academies should consider and choose those that are most suitable, given their particular circumstances.

An effective school/academy Online Safety Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school/academy community.

It is suggested that consultation in the production of this policy should involve:

- Governors/directors
- Teaching Staff and Support Staff
- Students/pupils
- Parents
- Community users and any other relevant groups.

Due to the ever changing nature of digital technologies, it is best practice that the school/academy reviews the Online Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Given the range of optional statements offered and the guidance notes provided, this template document is longer than the resulting school policy is likely to be. It is intended that, while covering a complicated and ever-changing aspect of the work of the school/academy, the resulting policy should be concise and easily understood, if it is to be effective and adopted by all.

The template uses a number of alternative terms e.g. Headteacher/Principal; Governors/directors; students/pupils; local authority/other responsible body. Schools/academies will need to choose which term is relevant and delete the other accordingly.

Within this template, sections which include information or guidance are shown in BLUE. It is anticipated that schools/academies would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in ITALICS it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in BOLD, it is suggested that these should be an essential part of a school/academy Online Safety Policy.

The first part of this document (approximately 25 pages) provides a template for an overall Online Safety Policy for the school/academy. The appendices contain more detailed and more specific policy templates and agreement forms. It will be for schools/academies to decide which of these documents they chose to amend and adopt.

Online Safety Policy
Marwood School
March 2022

Development/Monitoring/Review of this Policy

This online safety policy has been developed by Marwood Governors and Headteacher

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

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	*Insert date 23/03/22*
The implementation of this online safety policy will be monitored by:	*Alun Dobson and the Teaching and Learning Committee of Marwood Governors*
Monitoring will take place at regular intervals:	*Annually in the Spring Term*
The Board of Directors/Governing Body/Governors Sub Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually in the Spring Term*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually in the Spring Term*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA Safeguarding Officer, LADO, Police*

The school will monitor the impact of the policy using: *(delete/add as relevant)*

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- 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 *school/academy* community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school/academy digital technology systems, both in and out of the *school/academy*.

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

The *school/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 safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school/academy*:

Governors/Board of Directors

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

- regular meetings with the Online Safety Co-ordinator/officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting

Headteacher/Principal and Senior Leaders

- The *Headteacher/Principal* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Lead*.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority/MAT/other relevant body* disciplinary procedures
- *The Headteacher/Principal and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.*
- *The Headteacher/Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

Online Safety Lead – Alun Dobson

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/MAT/relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (Examples of suitable log sheets may be found later in this document). Online Safety BOOST includes access to Whisper, an anonymous reporting app that installs onto a school website and extends the schools ability to capture reports from staff, children and parents https://boost.swgfl.org.uk/
- meets regularly with Online Safety *Governor/Director* to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of *Governors/Directors*
- reports regularly to Senior Leadership Team

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the *school's/academy's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *school/academy* meets required online safety technical requirements and any *Local Authority/MAT/other relevant body* online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person* – Smoothwall in place
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *networks/internet/digital technologies* is regularly monitored in order that any misuse/attempted misuse can be reported to the *Headteacher/Principal and Senior Leaders; Online Safety Lead* for investigation/action/sanction
- *that monitoring software/systems are implemented and updated as agreed in school/academy policies*

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *school/academy* online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement (AUP/AUA)
- they report any suspected misuse or problem to the *Headteacher/* (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 safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned 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*

Designated Safeguarding Lead/Designated Person/Officer

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

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

Online Safety Group

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

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Lead (or other relevant person, as above) with:

- the production/review/monitoring of the school online safety 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 safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students/Pupils:

- are responsible for using the *school/academy* digital technology systems in accordance with the student/pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's/academy's* online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The *school/academy* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support the *school/academy* in promoting good online safety practice and to follow guidelines on the appropriate use of:

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

Community Users

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

Policy Statements

Education – Students/Pupils

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

In planning their online safety curriculum schools/academies may wish to refer to:

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- SWGfL Project Evolve – online safety curriculum programme and resources

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

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- *Students/pupils should be helped to understand the need for the student/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/academy.*
- *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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (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 safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school/academy will therefore seek to provide information and awareness to parents and carers through: (select/delete as appropriate)

- *Curriculum activities*
- *Letters, newsletters, web site, Learning Platform*
- *Parents/carers evenings/sessions*
- *High profile events/campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites/publications e.g.* swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers *(see appendix for further links/resources)*

Education – The Wider Community

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

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school/academy website will provide online safety information for the wider community*
- *Sharing their online safety expertise/good practice with other local schools*

- *Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool for groups such as these -* www.onlinecompass.org.uk

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select/delete as appropriate)

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. Online Safety BOOST includes unlimited online webinar training for all, or nominated, staff (https://boost.swgfl.org.uk/)
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements. Online Safety BOOST includes an array of presentations and resources that can be presented to new staff (https://boost.swgfl.org.uk/)
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.*
- *The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.* Online Safety BOOST includes an array of presentation resources that the Online Safety coordinator can access to deliver to staff https://boost.swgfl.org.uk/ It includes presenter notes to make it easy to confidently cascade to all staff

Training – Governors/Directors

Governors/Directors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school/academy training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

If the school/academy has a managed ICT service provided by an outside contractor, it is the responsibility of the school/academy to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school/academy, 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/MAT /other relevant body policies on these technical issues.

The school/academy will be responsible for ensuring that the school/academy 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 safety responsibilities: (schools/academies 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
- 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 *at KS2 and above* will be provided with a username and secure password by A Dobson *who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school/academy systems, 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/academy safe)
- J Hayward 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. Smoothwall is in place for filtering and updated against the CAIC list There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").
- *The school/academy has provided enhanced/differentiated user-level filtering* (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc)
- *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 may wish to add details of the monitoring programmes that are used).
- *An appropriate system is in place* (to be described) *for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).*
- Appropriate security measures are in place (schools/academies may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place 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 that allows staff to download executable files and installing programmes on school devices.*
- *An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices.* ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured – Egress switch is used to transfer SEN and other Data. Devon's approved file transfer process is also used.***

Mobile Technologies (including BYOD/BYOT)

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

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

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include: security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership. A range of mobile technology implementations is possible

For further reading, please refer to " NEN Technical Strategy Guidance Note 5 – Bring your own device"

A more detailed Mobile Technologies Template Policy can be found in the appendix. The school may however choose to include these aspects of their policy in a comprehensive acceptable use agreement, rather than in a separate Mobile Technologies Policy. It is suggested that the school should in this overall policy document outline the main points from their agreed policy. A checklist of points to be considered in included below.

- The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*By agreement*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*By agreement*
Internet only						
No network access						

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements:

School owned/provided devices:

- *Who they will be allocated to*
- *Where, when and how their use is allowed – times/places/in school/out of school*
- *If personal use is allowed*
- *Levels of access to networks/internet (as above)*
- *Management of devices/installation of apps/changing of settings/monitoring*
- *Network/broadband capacity*
- *Technical support*
- *Filtering of devices*
- *Access to cloud services*
- *Data Protection*

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- *Taking/storage/use of images*
- *Exit processes – what happens to devices/software/apps/stored data if user leaves the school*
- *Liability for damage*
- *Staff training*

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks/internet (as above)
- Network/broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
- Taking/storage/use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

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/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press – annual agreement by parents in place
- 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/academy 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/academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy 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/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the appendices to this document. Schools/academies should ensure that they take account of policies and guidance provided by local authorities/MAT/or other relevant bodies. For schools/academies that wish to carry out a more detailed review of their data protection policies and procedures SWGfL provides a self-review tool – 360data.org.uk

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

The school/academy must ensure that:

- it has a Data Protection Policy. (see appendix for template policy)
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school/academy may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)

- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school/academy, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected. (be sure to select devices that can be protected in this way)
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school/academy personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

(The school/academy will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.)

The Personal Data Advice and Guidance in the appendix provides more detailed information on the school's/academy's responsibilities and on good practice.

Communications

This is an area of rapidly developing technologies and uses. Schools/academies will need to discuss and agree how they intend to implement and use these technologies e.g. some schools do not allow students/pupils to use mobile

phones in lessons, while others recognise their educational potential and allow their use. This section may also be influenced by the age of the students/pupils. The table has been left blank for school/academy to choose its own responses.

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

The school/academy may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

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

- The official *school/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/pupils should therefore use only the school/academy email service to communicate with others when in school, or on school/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. (Online Safety BOOST includes an anonymous reporting app Whisper – https://boost.swgfl.org.uk/)

- Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, 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.*
- *Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above will be provided with individual school/academy email addresses for educational use.* (Schools/academies may choose to use group or class email addresses for younger age groups e.g. at KS1)
- *Students/pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school/academy website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school/academy and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school/academy protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools/academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

A more detailed Social Media Template Policy can be found in the appendix. The school/academy may however choose to include these aspects of their policy in a comprehensive acceptable use agreement, rather than in a separate Social Media Policy. It is suggested that the school/academy should, in this overall policy document, outline the main points from their agreed policy. A checklist of points to be considered is included below.

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

The school/academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. Online Safety BOOST includes unlimited webinar training on this subject: https://boost.swgfl.org.uk/
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School/academy staff should ensure that:

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

When official school/academy social media accounts are established there should be:

- *A process for approval by senior leaders*

- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school/academy disciplinary procedures*

Personal Use:

- 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/academy or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy 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/academy permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media:

- 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

The *school's/academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies. Online Safety BOOST includes Reputation Alerts that highlight any reference to the school/academy in online media (newspaper or social media for example) https://boost.swgfl.org.uk/)

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school/academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school/academy context, either because of the age of the users or the nature of those activities.

The school/academy believes that the activities referred to in the following section would be inappropriate in a school/academy context and that users, as defined below, should not engage in these activities in/or outside the school/academy when using school/academy equipment or systems. The school/academy 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	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X

sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools/academies will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	

Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce			X		
File sharing			X		
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

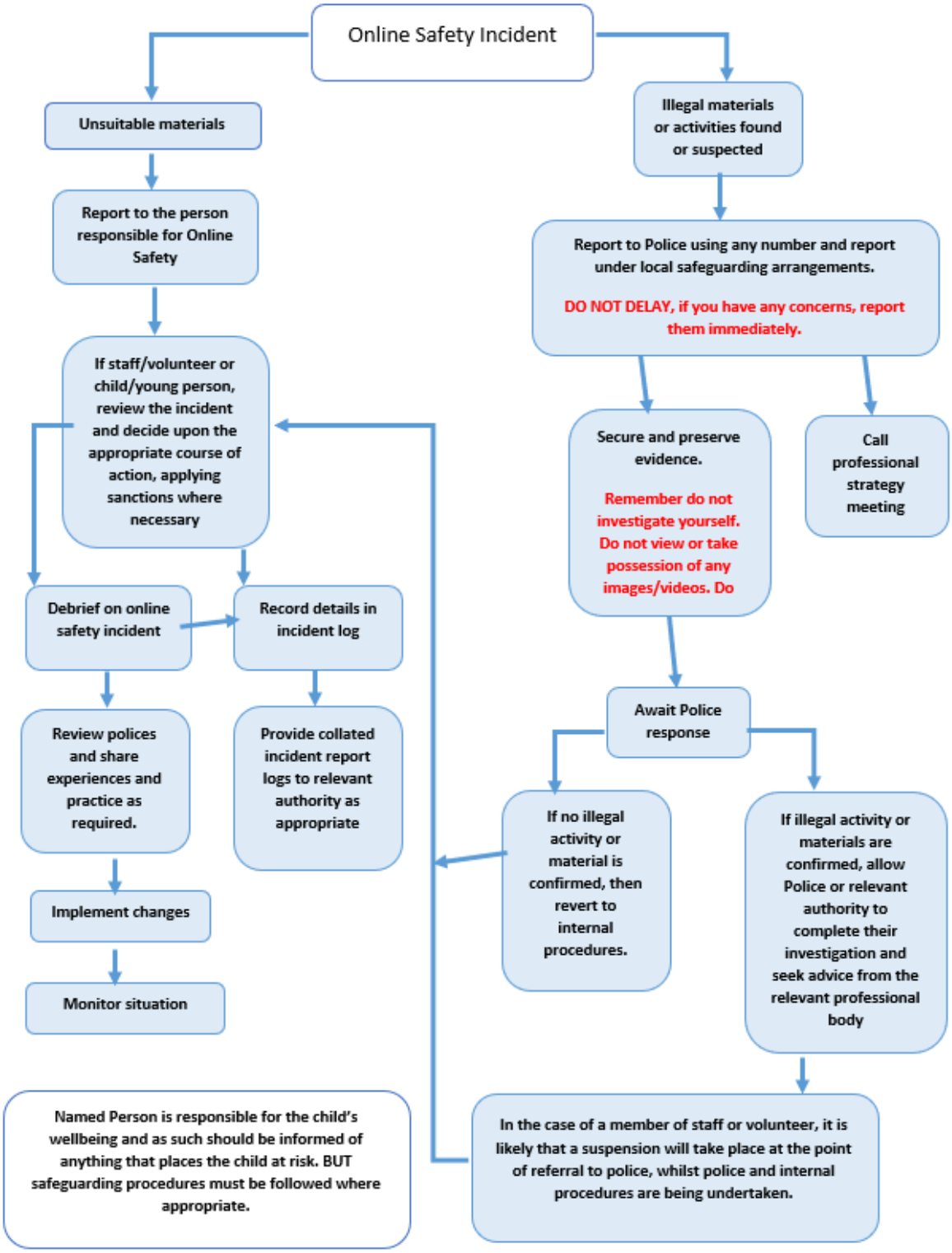
(The *school/academy* should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for *schools/academies* to decide their own responses)

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). Online Safety 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 (https://boost.swgfl.org.uk/)

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school/academy community will be responsible users of digital technologies, who understand and follow school/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 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/Academy Group 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
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School/academy actions & sanctions

It is more likely that the school/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 as follows: (the school/academy will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools/academies have found it useful to use the charts below at staff meetings/training sessions).

Students/Pupils Incidents	Actions/Sanctions								
	Refer to class teacher/tutor	Refer to Head of Department/Year/other	Refer to Headteacher/Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X		X		X	X		X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device			X			X		X	
Unauthorised/inappropriate use of social media/ messaging apps/personal email			X			X		X	
Unauthorised downloading or uploading of files			X		X	X		X	
Allowing others to access school/academy network by sharing username and passwords			X			X	X	X	
Attempting to access or accessing the school/academy network, using another student's/pupil's account			X			X	X	X	
Attempting to access or accessing the school/academy network, using the account of a member of staff			X			X	X	X	
Corrupting or destroying the data of other users			X			X	X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions			X			X	X		X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school			X			X	X		X
Using proxy sites or other means to subvert the school's/academy's filtering system			X		X	X	X		X

Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material			X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X		X	X	X	X	

Actions/Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email		X	X		X	X		X
Unauthorised downloading or uploading of files		X			X	X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner		X			X	X		X
Deliberate actions to breach data protection or network security rules		X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X

Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X	X		X			X
Actions which could compromise the staff member's professional standing		X	X		X			X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy		X			X			X
Using proxy sites or other means to subvert the school's/academy's filtering system		X	X		X			X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Breaching copyright or licensing regulations		X			X			X
Continued infringements of the above, following previous warnings or sanctions		X	X		X			X

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

SWGfL Online Safety Policy Templates

Acknowledgements

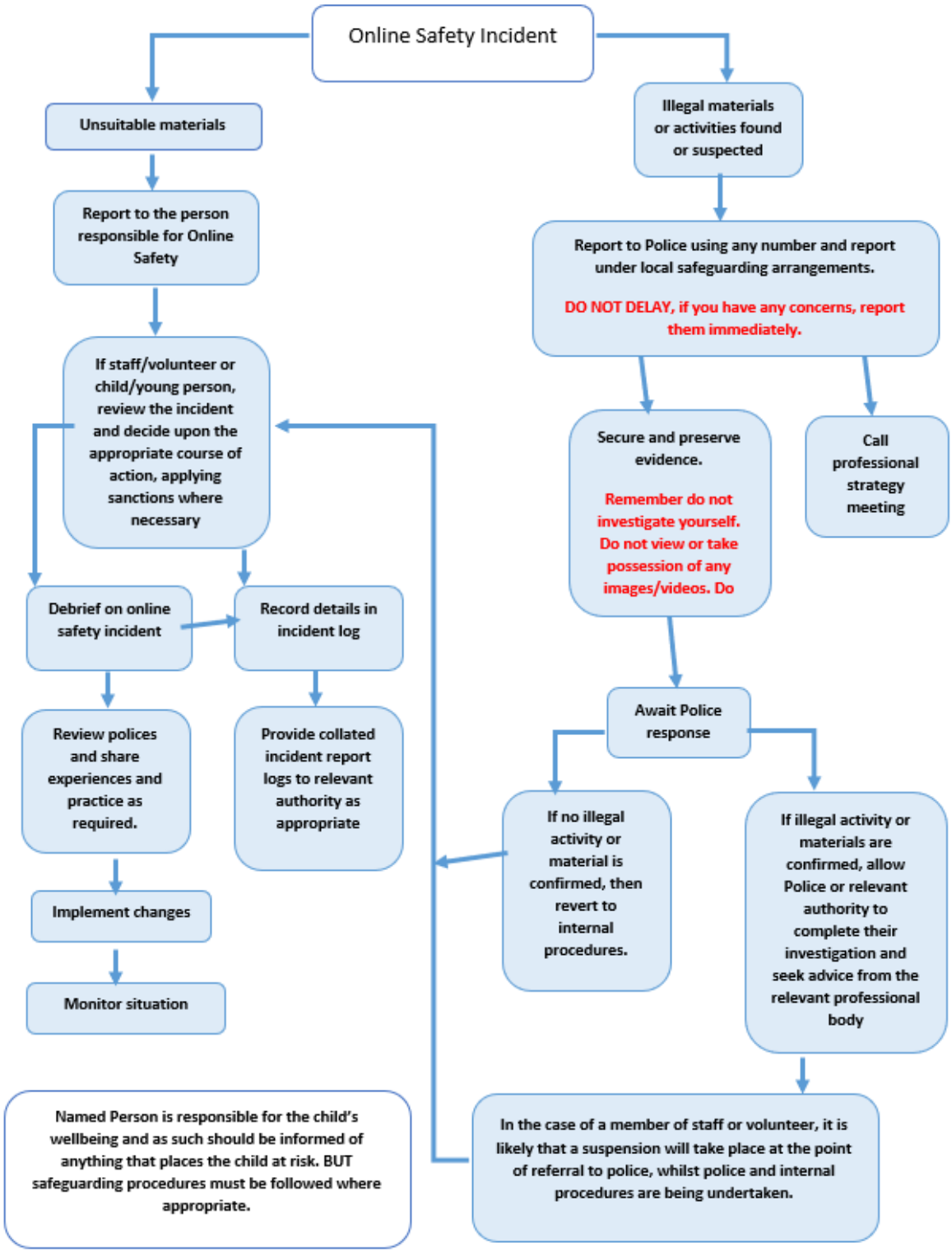
SWGfL would like to acknowledge the contribution of a wide range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the online safety policy templates and of the 360 degree safe online safety self-review tool.

Copyright of these template policies is held by SWGfL. Schools/academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2020

Responding to incidents of misuse – flow chart



Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Inci By
			What?	By Whom?	

Mobile Technologies Policy Template (inc. BYOD/BYOT)

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

The absolute key to considering the use of mobile technologies is that the pupils/students, staff and wider school/academy community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school/academy owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students/pupils that will prepare them for the high tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school/academy network, filtering of personal devices, breakages and

insurance, access to devices for all students/pupils, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools/academies may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school/academy community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school/academy embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of mobile technology implementations is possible. The school/academy should consider the following statements and remove those that do not apply to their planned implementation approach.

- The school/academy acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows: (the school/academy should complete the table below to indicate which devices are allowed and define their access to school/academy systems)

	School/academy/devices			Personal devices		
	School/academy owned and allocated to a single user	School/academy owned for use by multiple users	Authorised device[2]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes by agreement
Full network access	*Yes*	*Yes*	*Yes*	No	Yes	Yes by agreement
Internet only						
No network access						

- The school/academy has provided technical solutions for the safe use of mobile technology for school/academy devices/personal devices (delete/amend as appropriate):
    - All school/academy devices are controlled though the use of Mobile Device Management software

[2] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The school/academy has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school/academy location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- *All school/academy devices are subject to routine monitoring*
- *Pro-active monitoring has been implemented to monitor activity*

- *When personal devices are permitted:*
  - *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*
  - *Personal devices are brought into the school/academy entirely at the risk of the owner and the decision to bring the device in to the school/academy lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
  - *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
  - *The school/academy accepts no responsibility for any malfunction of a device due to changes made to the device while on the school/academy network or whilst resolving any connectivity issues*
  - *The school/academy recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
  - *The school/academy is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*
- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;
  - Devices may not be used in tests or exams
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
  - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in the school/academy
  - Personal devices should be charged before being brought to the school/academy as the charging of personal devices is not permitted during the school/academy day
  - Devices must be in silent mode on the school/academy site and on school buses
  - School/academy devices are provided to support learning. It is expected that pupils/students will bring devices to the school/academy as required.
  - Confiscation and searching (England) - the school/academy has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - The changing of settings (exceptions include personal settings such as font size, brightness, etc...) that would stop the device working as it was originally set up and intended to work is not permitted
  - The software/apps originally installed by the school/academy must remain on the school/academy owned device in usable condition and be easily accessible at all times. From time to time the

school/academy may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps

- The school/academy will ensure that devices contain the necessary apps for school/academy work. Apps added by the school/academy will remain the property of the school/academy and will not be accessible to students/pupils on authorised devices once they leave the school/academy roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- *Devices may be used in lessons in accordance with teacher direction*
- *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*
- *Printing from personal devices will not be possible*

Insurance

Schools/academies that have implemented an authorised device approach (1:1 deployment) may wish to consider how they will insure these devices and should include details of the claims process in this policy.

Social Media Policy Template

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/academy 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/academy*, its staff, parents, carers and children.

Scope

This policy is subject to the school's/academy'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/academy.
- 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/academy*

The school/academy 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/academy 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, or impacts on, the school/academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy 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/academy 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/academy 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/academy accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school/academy

Process for creating new accounts

The school/academy 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 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/academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school/academy, including volunteers or parents.

Monitoring

School/academy 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/academy social media account.

Behaviour

- The school/academy 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/academy 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/academy.
- 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/academy 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/academy 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/academy policies. *The school/academy 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/academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school/academy will deal with the matter internally. Where conduct is considered illegal, the school/academy 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/academy, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school/academy 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/academy 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/academy 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/academy'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/pupil pictures online other than via school/academy owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school/academy social media accounts. Students/pupils should be appropriately dressed, not be subject to ridicule and must not be on any school/academy 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/academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy 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/academy are outside the scope of this policy.
    - Where excessive personal use of social media in school/academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - *The school/academy 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/academy on any personal social media network account.
    - The school's/academy'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/academy. Any offensive or inappropriate comments will be resolved by the use of the school's/academy'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/academy 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/academy. In the event of any offensive or inappropriate comments being made, the school/academy 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/academy'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/academy.
- The school/academy 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/academy 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/academy 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/academy 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/academy 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.

Links to other organisations or documents

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

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

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/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

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 – Cyberbullying guidance and practical PSHE toolkit:

http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

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

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, 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
ICO	Information Commissioners Office
ICT	Information and Communications Technology
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
MAT	Multi Academy Trust
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.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.