



IT Online Safety and Online Safeguarding

Key Document Details

School Name:	The White Horse Federation – all schools	Ratified date:	September 2021
Version no:	8	Interim review date	n/a
Author:	S Cowley	Next review date:	September 2022
Owner:	M Weller		
Approved by:	CEO		

Scope of the Policy

This policy applies to all members of *The White Horse Federation (TWHF)* 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/TWHF*.

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* 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*, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online 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/TWHF*:

Board of Trustees

Trustees are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. The approval is delegated to the CEO. This will be carried out by Teaching and Standards *Sub Committee* receiving regular information about online safety incidents and monitoring reports. A member of the *Trustees* has taken on the role of *Online Safety Governor*.

Local Governing Board

The role of the LGB Safeguarding / *Online Safety Governor* 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 (SLT) 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 *MAT* disciplinary procedures). All TWHF schools use CPOMs for this purpose to log such incidents.
- 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 Computing Team have an overview of Online Safety monitoring schedule that they recommend for each school. All schools should use this overview.
- A member of the Senior Leadership Team will be part of this team and the SLT as a whole will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- 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 and are possible to build on CPOMs to monitor and audit incidents to keep them in one place) 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

The school will follow the same reporting route for inappropriate content taken from the SWGfL flow diagram in this policy. The Principal should lead on this having an overview of all incidents allowing any connections to be made.

Network Manager/Technical staff

(N.B. Two schools have a managed ICT service provided by an outside contractor. It is the responsibility of the *school* to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the MATs technical staff, as suggested below. It is also important that the managed service provider is fully aware of the *school's* online safety policy and procedures.)

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* (see appendix "Technical Security Policy Template" for good practice)
- 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/Principal/Senior Leader/Online Safety Lead* 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

N.B. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

It is key that the Designated Safeguarding Lead and Online Safety Lead have clear and frequent lines of communications.

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

Schools will need to decide the membership of the Online Safety Group. It is recommended that the group should include representation from students/pupils and parents/carers).

An Online Safety Group Terms of Reference Template can be found in the appendices.

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 our online safety curriculum schools/academies refer to:

- [DfE Teaching Online Safety in Schools](#)
- [Education for a Connected World 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 is 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 relevant 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 at an age appropriate level.
 - 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.

these are 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.

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:

- *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>*

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 (This may be a via range of activities including website links, parent evening demonstration, newsletters etc.)
- 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:

- 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.
- 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.
- 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.

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 MAT/ Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school/academy training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school/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 pupil users have a 365 log in provided by Network Managers.
- 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)
- The Procurement Manager and IT Director are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.
- 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. The MAT use the filtering and firewall on the CAIC and is updated regularly. 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. These are 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 MAT 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.
- 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/forbids staff from downloading 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. (see School Personal Data Policy Template in the appendix for further detail)

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 policies 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.

For further reading, please refer to “ [NEN Technical Strategy Guidance Note 5 – Bring your own device](#)” and TWHF BYOD Policy.

- The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- All non TWHF devices can only be connected to the Guest Wifi services and will not have direct access to TWHF networks.

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
- 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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *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. 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. ([The White Horse Federation - GDPR](#))
- 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 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 White Horse Federation - GDPR](#)).
- 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. This is outlined on the [The White Horse Federation - GDPR](#)
- 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 ([The White Horse Federation - GDPR](#)) (see also 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 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.
- 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 understand 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

At present the MAT only allows data storage on removal media if encrypted.

Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree at a local level how they intend to implement and use these technologies and will be influenced by the age of the students/pupils. 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.

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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 and should be aligned to existing online communications policy
- <https://thewhitehorsefederation.org.uk/downloads/default/The-White-Horse-Federation-%E2%80%93-Communications-Policy-SOPs.pdf>

- 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.
- Due to Home Learning during Covid, all pupils have individual 365 accounts.
- 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

Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that are in place to intervene and support should a particular issue arise. Schools 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 overview can be found in the Acceptable User Agreement and Social Media Policy.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff.

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School/academy staff should ensure that:

- No reference should be made in social media to students/pupils, parents/carers or school/academy staff beyond what is already in the public domain e.g. newspaper articles, school websites
- 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* /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 an awareness of the procedures to be followed around social media account management as detailed in the Social Media Accounts Policy including:

- 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:

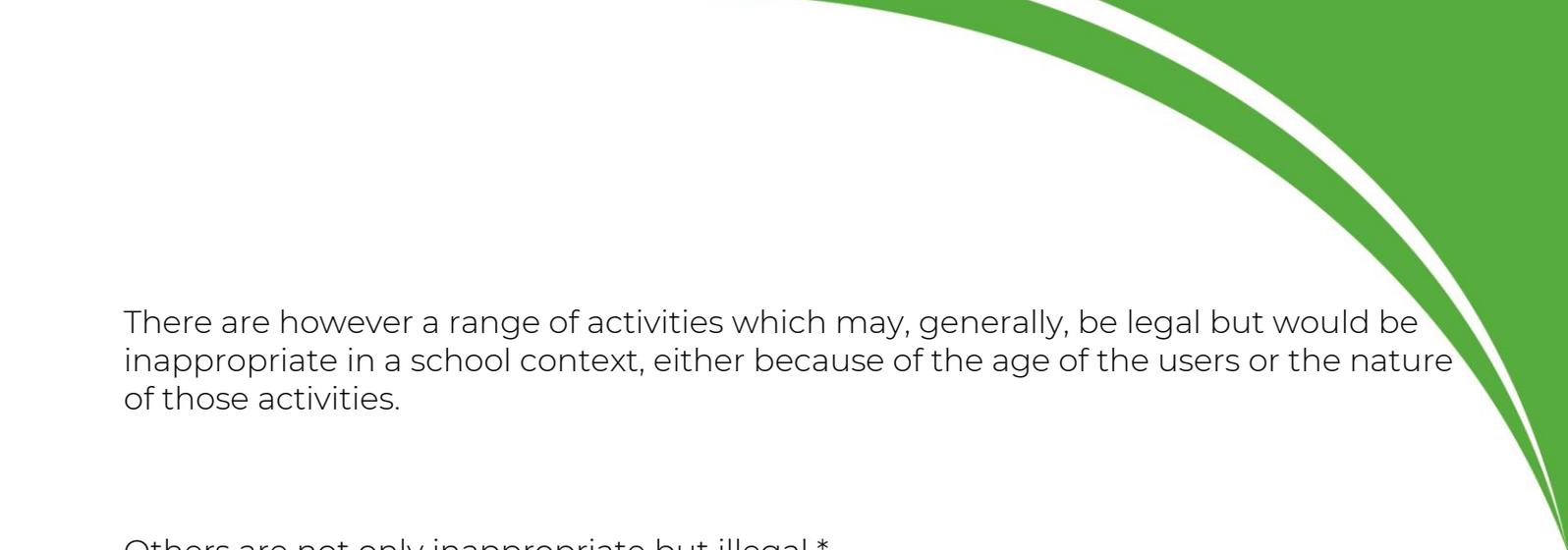
- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

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* 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. Eduprise can support here by producing online 'sentiment reports' for existing social media platforms alongside usage.

Dealing with unsuitable/inappropriate activities:



There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Others are not only inappropriate but illegal *

TWHF 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 when using school equipment or systems.

The school/MAT policy restricts usage as follows:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. 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. *
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 *
- 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 *
- Pornography
- Promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- 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

Activities that might be classed as cyber-crime under the Computer Misuse Act:

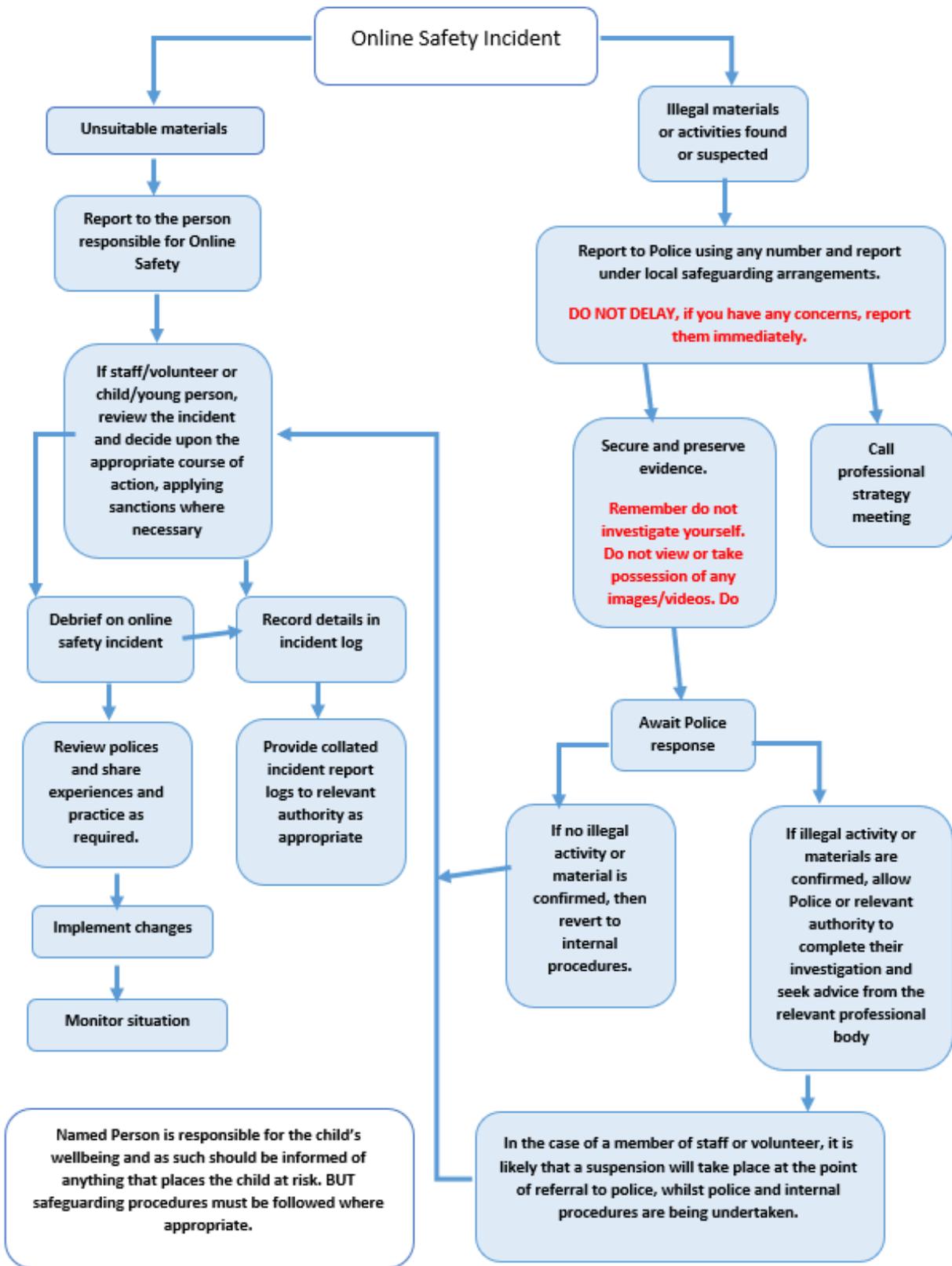
- Gaining unauthorised access to school networks, data and files, through the use of computers/devices *
- Creating or propagating computer viruses or other harmful files *
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) *
- Disable/Impair/Disrupt network functionality through the use of computers/devices *
- Using penetration testing equipment (without relevant permission) *
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Unfair usage (downloading/uploading large files that hinders others in their use of the internet)
- Using school systems to run a private business
- Infringing copyright
- On-line gambling
- On-line shopping/commerce
- Use of social media
- Use of messaging apps
- Use of video broadcasting e.g. YouTube

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).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or 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 expected that all members of the school 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/MAT* - and possibly the police - and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be

retained by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Acknowledgements

This Online Safety and Online Safeguarding Policy is based on a policy template from SWGfL.