TOR VIEW
A SPECIALIST LEARNING COMMUNITY

ONLINE SAFEGUARDING POLICY

Development / Monitoring / Review of this Policy

This Online Safeguarding policy has been developed by the Deputy Headteacher (Curriculum & Quality)

- Headteacher / Senior Leaders
- Online Safeguarding Lead – KM (Deputy Headteacher – DSL)
- Online Safeguarding Team – KM JP AOB CM PE & Online Leaders
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents and Carers
- Community users

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 Safeguarding policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	*Autumn 2019*
The implementation of this Online Safety policy will be monitored by the:	*Headteacher, Senior Leadership Team and Online Safety Lead*
Monitoring will take place at regular intervals:	*Monitoring will take place across the academic year.*
The Board of Directors / Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safeguarding Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*The Governors will be updated 3 times a year within governor's meetings (or more frequently when necessary). Chair of Governors will sign any Online Safeguarding issues within these meetings.*
The Online Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safeguarding or incidents that have taken place. The next anticipated review date will be:	*Summer each year and updated throughout the year in accordance with any updated national documentation.*

Should serious online safeguarding incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, Academy Group Officials, LADO, Police*

The school will monitor the impact of the policy using:

- 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

Scope of the Policy

Online Safeguarding must:

Protect and educate pupils and staff in their use of technology, and have the appropriate mechanisms to intervene and support incidents where appropriate.

The breadth of issues classified within Online Safeguarding are considerable but can be categorised into three areas:

Content: Being exposes to illegal, inappropriate or harmful material.

Contact: Being subjected to harmful online interaction with other users.

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm.

- This policy applies to all members of the school / academy community (including staff, governors/trustees, 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 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 consequences in line with the conduct policy for inappropriate conduct. This is pertinent to incidents of online-bullying or other Online Safeguarding incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the school / academy.

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

Roles and Responsibilities

It is everyone's responsibility to ensure policy and procedures are understood and respected by all at all times.

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

Please see September 2019 further notes KSCIE (2019) Online Safety.

Governors

Governors are responsible for the approval of the Online Safeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safeguarding incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safeguarding Governor – Ellie Lorenzo – Chair of Governors.

The role of the Online Safeguarding Governor will include:

- Regular meetings with the Online Safeguarding Lead
- Attendance at some Online Safeguarding meetings with the Online Safeguarding Team.
- Regular monitoring of Online Safeguarding incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including Online Safeguarding) of members of the school community, though the day to day responsibility for Online Safeguarding will be delegated to the Online Safety Lead and Online Safeguarding Team.

- The Headteacher and all members of the Senior Management Team should be aware of the procedures to be followed in the event of a serious Online Safeguarding allegation being made against a member of staff**. (Please see flow chart on dealing with online safeguarding incidents)**

- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safeguarding 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 and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safeguarding monitoring role. This is to provide a safety net and also to support to those colleagues who take on important monitoring roles.

- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

It is strongly recommended that each school should have a named member of staff with a day to day responsibility for Online Safeguarding, some schools may choose to combine this with the Designated Safeguarding Lead role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school

- Leads the Online Safeguarding Team
- Takes day to day responsibility for Online Safeguarding issues and has a leading role in establishing and reviewing the school Online Safeguarding policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safeguarding incident taking place.
- Organises training and advice for staff:
- Tor View ensures annual Online Safeguarding training for all stakeholders and regular training across the academic year to reflect current research and advance in technology.
- An Online Safeguarding Team is identified within school with a responsibility for Online Safeguarding. Within the Online Safeguarding Team there are members with a higher level of expertise and clearly defined responsibilities.
- Liaises with the Local Authority / MAT / relevant body
- Liaises with school technical staff

- Receives reports of Online Safeguarding incidents and creates a log of incidents to inform future Online Safeguarding developments. (All copies kept in the Online Safeguarding file or on CPOMS)

- Meets regularly with Online Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of *Governors*
- Reports weekly to Senior Leadership Team, reports weekly to the Senior Management team, reports termly to the governors.
- Any incidents or changes to practice are distributed through Assistant Headteachers in weekly departmental briefings.

The school will need to decide how these incidents will be dealt with and whether the investigation / action / sanctions will be the responsibility of the Online Safeguarding Lead or another member of staff e.g. Headteacher / Senior Leader / Designated Safeguarding Lead / Class teacher / Head of Department.)

Network Manager / Technical staff

(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 safeguarding measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school / academy Online Safeguarding Policy and procedures.)

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is 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, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (Please see Tor View Filtering Policy)
- That they keep up to date with Online Safeguarding 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 network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher /Senior Leader; 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 Safeguarding matters and of the current school / academy Online Safeguarding Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher / Senior Leader ; Online Safeguarding 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 Safeguarding issues are embedded in all aspects of the curriculum and other activities
- Students / pupils understand and follow the Online Safeguarding Policy and acceptable use policies. (Please see posters for pupils)
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. (Where appropriate)
- 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

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

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online-bullying

(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. Some schools may choose to combine the roles of Designated Safeguarding Lead and Online Safety Lead)

Online Safeguarding Team

The Online Safeguarding Team provides a consultative group that has wide representation from the school / academy community, with responsibility for issues regarding online safeguarding and the monitoring the Online Safeguarding Policy including the impact of initiatives. Depending on the size or structure of the school / 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 Safeguarding Group will assist the Online Safety Lead (or other relevant person, as above) with:

- The production / review / monitoring of the school Online Safeguarding Policy / documents.
- The production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- Mapping and reviewing the online safeguarding / digital literacy curricular provision – ensuring relevance, breadth and progression
- Monitoring network / internet / incident logs
- Consulting stakeholders – including parents / carers and the students / pupils about the online safety provision

The Online Safeguarding Team consists of DSL Deputy Headteacher, Assistant Headteacher, Lead Teacher, Teacher, ICT Technician and Online Leaders.

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 (Where appropriate)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. *The mechanisms school have in place to support pupil facing online safety issues:* Tor View encourage pupils to tell an adult if they have any concerns, and visual posters in classrooms further promote this. Tor View pupils may also report any concerns to the Online Leaders. (See Appendix 5 – Reporting Online Safeguarding for Pupils)

- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- Should understand the importance of adopting good Online Safeguarding practice when using digital technologies out of school and realise that the school's / academy's Online

Safeguarding Policy covers their actions out of school, if related to their membership of the school.

Tor View have representatives from across school that meet fortnightly as an Online Leader. This group is facilitated by a member of SMT to discuss issues and distribute information to their peers. During these meetings views can be taken from the representatives in relation to Online Safeguarding.

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 / and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school / academy in promoting good online safeguarding practice and to follow guidelines on the appropriate use of:

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

Tor View strive to ensure parents are kept up to date with the most recent changes in Online Safeguarding.

Community Users

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

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 Safeguarding / digital literacy is therefore an essential part of the school's / academy's Online Safeguarding provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

- Online Safeguarding should be a focus in all areas of the curriculum and staff should reinforce Online Safeguarding messages across the curriculum. The Online Safeguarding curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: *(statements will need to be adapted, depending on school / academy structure and the age of the students / pupils)*

- A planned online safeguarding curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited. (Please see updates to PHSCE curriculum)

- Key Online Safeguarding 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. *(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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safeguarding risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's 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.*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications*
- As a school we work closely with parents and carers to ensure their children use technology safely and responsibly at home and at school. We have a Parent Liaison Officer within school that also works alongside families and the Online Safeguarding Lead.

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 safeguarding knowledge and experience. This may be offered through the following:

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

As a school we regularly provide updates and training regarding Online Safeguarding to improve all stakeholder's knowledge of and expertise in the safe and appropriate use of technologies.

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safeguarding training will be made available to staff annually alongside safeguarding training. This will be regularly updated and reinforced.

- An audit of the online safety training needs of all staff will be carried out regularly by the Online Safeguarding Team.

- All new staff should receive online safeguarding training as part of their induction programme (Safeguarding Training) ensuring that they fully understand the school / academy Online Safeguarding Policy and Acceptable Use Agreements.

- It is expected that some staff will identify online safeguarding as a training need within the appraisal process.

- The Online Safeguarding Team will receive regular updates through attendance at external training events.

- This Online Safeguarding Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

- The Online Safeguarding Lead will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority.

- Participation in school / academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

- Technical – infrastructure / equipment, filtering and monitoring (Please see Filtering and Monitoring documents)

- *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 safeguarding 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 Safeguarding 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 (these may be outlined in Local Authority / MAT / other relevant body policy and guidance)

- There will be regular reviews and audits of the safety and security of school / academy technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school / academy technical systems and devices.

- We choose to use group or class log-ons and passwords for some classes.

- The "master / administrator" passwords for the school / academy ICT systems, used by the Network Manager (or other person) are available to the *Headteacher /*Online Safeguarding Lead and kept in a secure place (school / academy safe)

- The ICT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations *(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. 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. *(Additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 requires schools / academies to ensure that children are safe from terrorist and extremist material on the internet.*

- 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.

- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. Staff report this to the Technical Team/Leadership Team or Online Safeguarding Lead.

- Appropriate security measures are in place *(schools / academies may wish to provide more detail – See Appendix 7 Risk Assessment)* 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 workstations are protected by up to date virus software.

- An agreed Community Acceptable Use Policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that forbids staff from downloading executable files and installing programmes on school devices.

- It is agreed that the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices is not permitted. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (Highlighted in School GDPR Policy)

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, Conduct Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and. appropriate use of mobile technologies should be an integral part of the school's Online Safeguarding education curriculum.

The school 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.

- The school Acceptable Use Agreements for staff, pupils/students and parents / carers/community users will give consideration to the use of mobile technologies

	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[2]*	*Yes[2]*	*Yes[2]*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only (Filtered)	*Yes*	*Yes*	*Yes*	*No*	*No*	*Yes*
No network access	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Aspects that the school may wish to consider and be included in their Online Safeguarding 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*
- *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)

[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.

[2] **The school should add below any specific requirements about the use of mobile / personal devices in school**

- Restrictions on where, when and how they may be used in school (all visitors are asked to turn off their mobile phones before entering the building and sign an acceptable use policy when they sign in) (Students and volunteers that are on site for short periods of time are instructed to hand mobile phones into the main office during the induction process)
- Storage (All staff are allocated lockers for their personal belongings, which includes mobile phones) (All pupil mobile phones are handed into a designated member of staff on arrival and signed back out to the pupil on departure)
- 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 Safeguarding 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 cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
- When using digital images, staff should inform and educate students / 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 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 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 change following the European Union General Data Protection Regulation (GDPR) announced in 2016. As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data.

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.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO). The school / academy may also wish to appoint a Data Manager and systems controllers to support the DPO.

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

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- The data must be encrypted and password protected.

- The device must be password protected. *(many memory sticks / cards and other mobile devices cannot be password protected)*
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school / academy policy once it has been transferred or its use is complete.

(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.)

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 eg 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.

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	cked away in lockers, office.	Allowed at certain times	Allowed for selected staff	Not allowed	wed: Handed in at reception	Allowed at certain times	llowed with staff permission	Not allowed
Mobile phones may be brought to the school / academy	x	x	x		x			
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones / cameras			x					x
Use of other mobile devices e.g. tablets, gaming devices		x	x			x		
Use of personal email addresses in school / academy , or on school / academy network				x				x

Use of school / academy email for personal emails				x				x
Use of messaging apps		x						x
Use of social media		x						x
Use of blogs		x						x

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.
- 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.
- Students / pupils should be taught about Online Safeguarding issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- 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
- 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*
- *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 Safeguarding Group to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / 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	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	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	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	

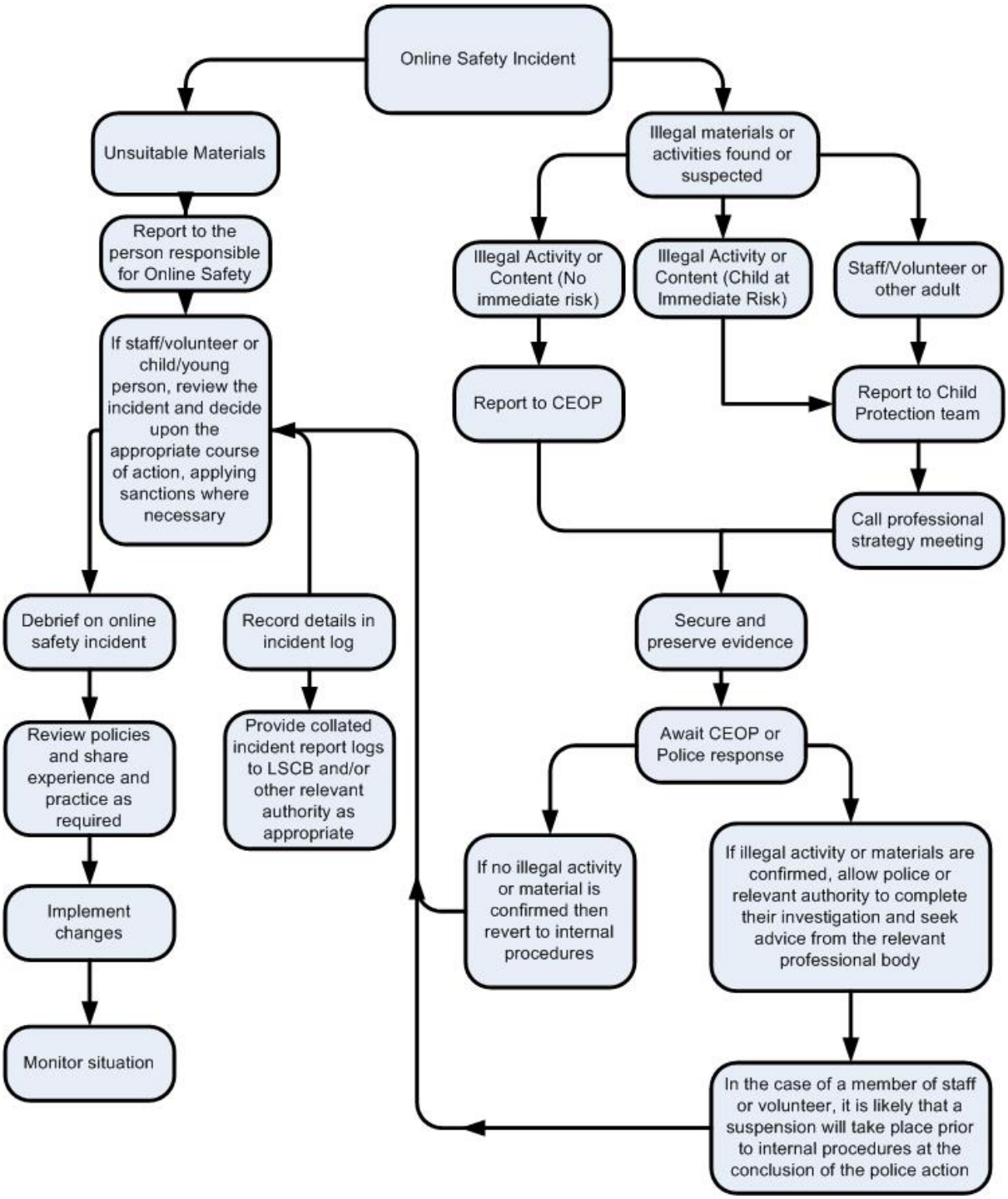
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		x			
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping / commerce				x	
File sharing					x
Use of social media				x	
Use of messaging apps				x	
Use of video broadcasting e.g. Youtube		x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

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
    - 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:

Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year /	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	Warning	Further sanction eg detention /
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				
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x	x	x		x				
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x							
Unauthorised downloading or uploading of files	x	x			x				
Allowing others to access school / academy network by sharing username and passwords		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		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	x	x		
Continued infringements of the above, following previous warnings or sanctions		x	x		x	x		x	
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school			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	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		x		

Actions / Sanctions

Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	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		
Unauthorised downloading or uploading of files	x	x	x	x	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	x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	x		x	x	x	x
Deliberate actions to breach data protection or network security rules	x	x			x	x	x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x		x	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	x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	x	X	X	X	X	X	X	x
Actions which could compromise the staff member's professional standing	x	x			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	X	X	x
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X			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	X	x
Breaching copyright or licensing regulations	X	X	X	X	X	X	X	x
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X	x

Useful Documents:

1. KSCIE
2. Incident Flow Charts
3. Filtering Policy
4. Pupil Information – Key Features of Good Practice
5. Updates to PHSCE curriculum
6. Monitoring Policy
7. Risk Assessment

Acknowledgements

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.