



Part of **GIPPESWYK COMMUNITY EDUCATIONAL TRUST**

*Achieving success together*

This Policy has been adopted and approved by Gippswyk Community Educational Trust and has been adapted for use by Copleston High School.

<b>ONLINE SAFETY POLICY</b>	
Reviewed/Amended	May 2021
Ratified by Copleston LGB	30.6.21
Date of next Review	Summer Term 2022
Responsible Officer	ICT Systems Manager – Charles Greig / DSL – Mr H Palmer / ADSL Mrs Crofton Sleigh
Policy Number	CS14

## Contents

Aims and Purpose	2
Development/Monitoring/Review of this Policy	3
Scope of the policy	4
Roles and Responsibilities	5
Policy statements	9
Education and training	11
Technical- Infrastructure /equipment, filtering and monitoring	13
Data Protection	18
Communications	21
Social media	23
Categories of abuse/incidents	26
Examples of illegal and or inappropriate use	28
Responding to incidents of misuse	30
Other Incidents	31

<b>School actions &amp; sanctions for dealing with misuse</b>	<b>32</b>
Appendices Appendices	
Record of reviewing and logging	34
Social Media Policy	35
School Policy – Online Safety Group Terms of Reference	41
Legislation	44
Glossary of Terms	52
Parent guides	54

## **Aims and Purpose**

Copleston High School Online Safety Policy is a suitable document which considers all current and relevant issues, in a whole school context, linking with other relevant policies, such as the safeguarding, behaviour and anti-bullying policies.

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

The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

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

Revised "Keeping Children Safe in Education" guidance obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"

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

The first part of this document provides the overall Online Safety Policy for Copleston High school. The appendices contain the school Social Media Policy, legislation and useful guides for parents.

## **Online Safety Policy; Development/Monitoring/Review of this Policy**

This online safety policy has been developed by

- Principal and senior leaders
- Online Safety Lead
- Governors

Should serious online safety incidents take place, the following external persons/agencies should be informed:

DSL/ADSL

MASH

LA Safeguarding Officer

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, parents/carers and school staff

## **Scope of the Policy**

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

The Education and Inspections Act 2006 empowers the Principal to such extent as is reasonable, to regulate the behaviour of students 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. 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:

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor, this role is combined with that of the Safeguarding Governor (Sarah Anderson).

### **The role of the Online Safety Governor/Director will include:**

- Regular meetings with the Online Safety Lead
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to Governors

### **Principal and Senior Leaders:**

- The 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 Principal and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse”).
- The 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 Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

### **Online Safety Lead**

- 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, Governing body, MAT
- 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 are in the appendices but Copleston High School will use My Concern to log and review).
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends any relevant meetings of Governors
- Reports regularly to Senior Leadership Team

### Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school 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
- 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 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
- They report any suspected misuse or problem to the Principal/Senior Leader/Online Safety Lead for investigation/action/sanction
- All digital communications with students/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 understand and follow the Online Safety Policy and acceptable use policies

- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students 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 (DSL)

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. these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop. Unless the DSL and Online safety lead are the same person.

### Online Safety Group (the safeguarding team)

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body/Directors.

Members of the Online Safety Group will assist the Online Safety Lead with

- The production/review/monitoring of the school online safety policy/documents.
- The production/review/monitoring of the school filtering policy (if we choose 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 about the online safety provision
- Monitoring improvement actions identified through use of the self-review tool

## Students/Pupils:

- Are responsible for using the school digital technology systems in accordance with the student 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 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 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 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 school website, Go 4 Schools regarding on-line student records and data
- Their children's personal devices in the school

## Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school/academy systems. (A community users acceptable use agreement template can be found in the appendices.)

## **Policy Statements**

### Education – Students/Pupils

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

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

- DfE Teaching Online Safety in Schools
- Education for a Connected 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 should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Students should be helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students 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 are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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 and training of key groups/ stakeholders

### 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 will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- 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](http://swgfl.org.uk), [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/), <http://www.childnet.com/parents-and-carers> (see appendix for further links/resources)

### The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school 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

### 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 annual 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 will receive regular updates through attendance at external training events 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 will provide advice/guidance/training to individuals as required.

### Governors

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

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

## **Technical – infrastructure/equipment, filtering and monitoring**

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy/acceptable use agreements. The school should also check their Local Authority/MAT /other relevant body policies on these technical issues.

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.

- School technical systems will be managed in ways that ensure that the school 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 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 technical systems and devices.
- All users will be provided with a username and secure password by the school IT team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master/administrator” passwords for the school systems, used by the IT Manager, must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. school safe)
- IT 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. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.
- The school 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 technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.)

- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- Appropriate security measures are in place 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

### Mobile Technologies (including Bring Your Own Device)

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.

A checklist of points to be familiar with-

- The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- Table below indicate which devices are allowed and define access to school systems

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device <sup>1</sup>	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes- mobile phone	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	No	No	No	Yes (6 <sup>th</sup> form)	Yes	Yes
No network access	No	No	No	Yes	Yes	Yes

Aspects included in online safety policy, mobile technologies policy or acceptable use agreements:

School owned/provided devices:

- Who they will be allocated to
- Where, when and how their use is allowed – times/places/in school/out of school
- If personal use is allowed
- Levels of access to networks/internet (as above)
- Management of devices/installation of apps/changing of settings/monitoring
- Network/broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking/storage/use of images
- Exit processes – what happens to devices/software/apps/stored data if user leaves the school
- Liability for damage
- Staff training

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)

- Restrictions on where, when and how they may be used in school, if wishing to use a personal device whilst in school, this must not be using the school network at any time
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks/internet (as above)
- Network/broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search users devices in the case of misuse
- Taking/storage/use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

### Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet.

Such images may provide avenues for 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 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 are published on the school website/social media/local press (This is with the AUA signed by parents or carers at the start of the academic year - see parents/carers acceptable use agreement in the appendix)

- *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 are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Students work can only be published with the permission of the student 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).

More detailed guidance is available in the appendices to this document.

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

The school ensures that the following are in place-

- iData Protection Policy.
- Implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- Payment of the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- Appointed appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- '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
- 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
- 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. 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
- Provides staff, parents, and volunteers, students with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- Procedures in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

- Have undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- Understands how to share data lawfully and safely with other relevant data controllers.
- 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.
- 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 protected by an adequate password.
- 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: *(may wish to include more detail about their own data/password/encryption/secure transfer processes)*

- 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

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

## Communications

This is an area of rapidly developing technologies and uses.

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:

Communication Technologies	Staff & other adults				Students/Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	To be used at break and lunch outside only	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	X				X	X		
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X				X	X		
Taking photos on mobile phones/cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices				X				X
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of messaging apps		X			X	X		X
Use of social media		X				X		
Use of blogs		X				X		

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students in KS3 and above will be provided with individual school email addresses for educational use
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school/academy website and only official email addresses should be used to identify members of staff.

## **Social Media - Protecting Professional Identity**

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school 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 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 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 Policy can be found in the appendix.

Copleston High School have a duty of care to provide a safe learning environment for pupils and staff. 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

### **Social media- A guide for School staff:**

- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school, 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 social media accounts are established or where staff are planning to create a school account, there should be:

- ICT Manager to be informed prior to its creation. In addition they must adhere to the rules regarding safeguarding when posting content online. Any concerns regarding content posted will be passed on to the designated safeguarding lead and followed up accordingly.

- 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 disciplinary procedures

### **Personal Use:**

**Social networking outside of work hours**, on non-school/education setting or other establishment-issue equipment, is the personal choice of all staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Staff/Governors/Volunteers should ensure that personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with current students outside of Academy authorised systems (e.g. school email account for homework purposes). Specifically, staff must not be friends on Facebook or any other social networking sites such as Twitter with any current or ex –student of Copleston High School who is under the age of 20.  
There will be extreme exceptions (e.g. An ex-student becoming a colleague) in this circumstance it is the responsibility of the individual to ensure that the content on the social networking site is appropriate.
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a **professional** level. Some school/education setting or other establishments, other educational and other settings have set up accounts on Facebook to manage and monitor public and pupil communications through designated members of staff.
- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

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 schools 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.

## **Categories of abuse/ incidents**

### **CHILD EXPLOITATION AND E-SAFETY**

Children and young people can be exploited and suffer bullying through their use of modern technology such as the internet, mobile phones and social networking sites. In order to minimise the risks to our children and young people, Copleston High School and Sixth Form will ensure that we have in place appropriate measures such as security filtering, and an acceptable use policy linked to our e-Safety policy. We will ensure that staff are aware of how not to compromise their position of trust in or outside of the school and are aware of the dangers associated with the internet and other mobile technology.

Our ICT Acceptable Use and Mobile phone policy, in conjunction with our e-safety policy will clearly state that mobile phone or electronic communications with a student at our school is not acceptable other than for approved school business e.g. coursework, mentoring. Where it is suspected that a child is at risk from internet abuse or cyber bullying we will report our concerns to the appropriate agency. We will follow the e-safety flow chart in this policy to follow up and report incidents of e-safety.

### **CYBERBULLYING**

Cyberbullying, like all forms of bullying, is not tolerated at Copleston High School and Sixth Form. Cyberbullying will be investigated using our procedures as laid out in our Anti-Bullying Policy. Furthermore, we will use the e-safety flow chart to follow up incidents, where appropriate. Please refer to our Safeguarding and our Anti-Bullying Policies.

### **SEXTING**

The school will deal with incidents of sexting in line with the guidance and procedures set out in the UK Council for Child Internet Safety 'Sexting in schools and colleges: Responding to incidents and safeguarding young people' document.

### **SOCIAL NETWORKS**

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service offers users both a public and private space through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed.

With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, Twitter and Instagram).

In response to this issue the following measures have been put in place:

- Copleston High School controls access to social networking sites through existing filtering systems.
- Students are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school/education setting or other establishment name, groups or clubs attended, IM and email address or full names of friends).
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school/education setting or other establishment uniform).
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The school/education setting or other establishment should be aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the school/education setting or other establishment allowing for the procedures, as set out in the anti-bullying policy, to be followed.

## Examples of illegal and /or inappropriate use

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school 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 context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	

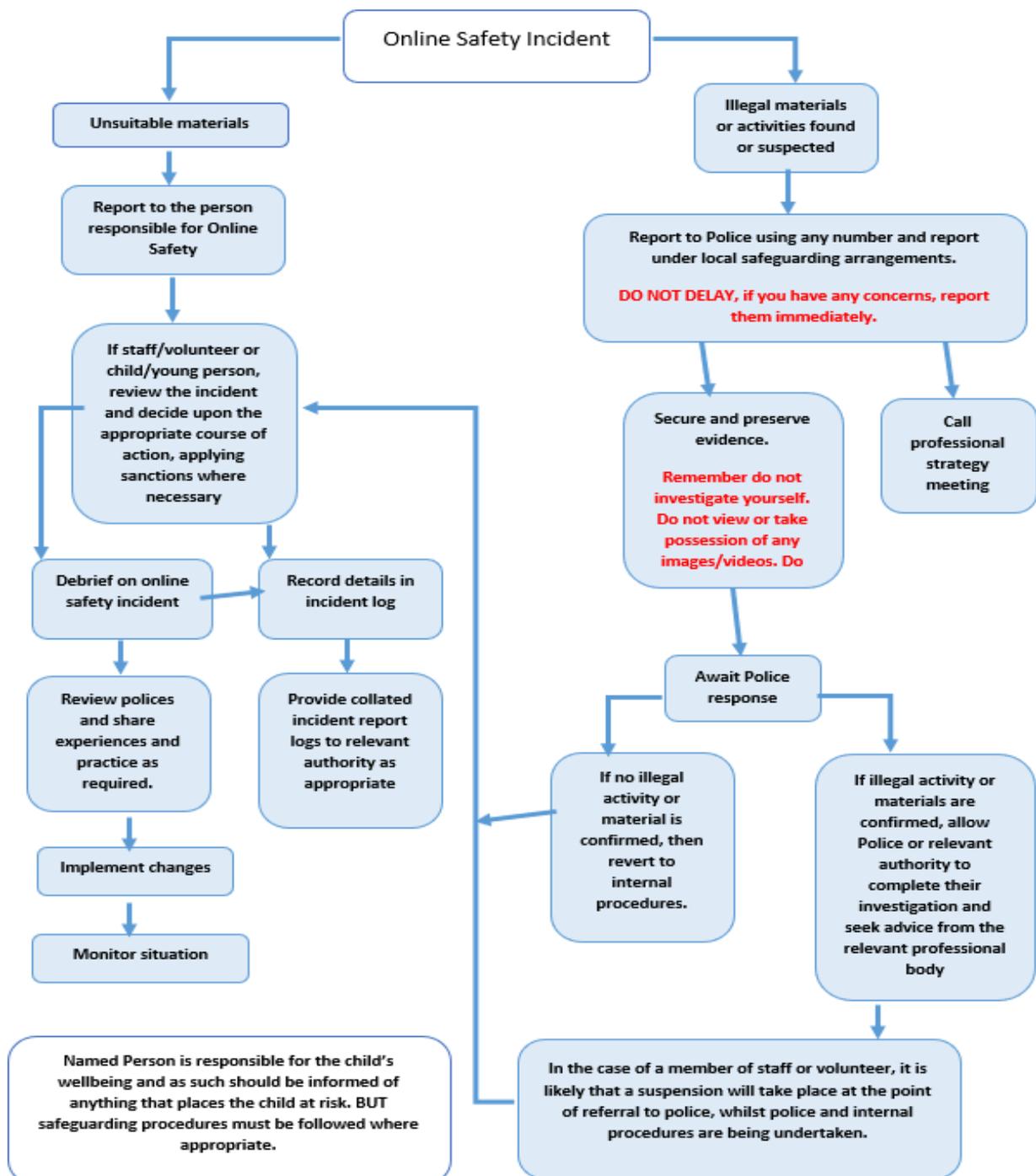
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
<p>Activities that might be classed as cyber-crime under the Computer Misuse Act:</p> <ul style="list-style-type: none"> <li>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>• Creating or propagating computer viruses or other harmful files</li> <li>• Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)</li> <li>• Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>• Using penetration testing equipment (without relevant permission)</li> </ul>					X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce				X	
File sharing				X	
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube				X	

## 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 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

All members of the school community will be responsible users of digital technologies, who understand and follow school 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
  - 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.
- *Sharing nudes and semi-nudes In the latest advice for schools and colleges (UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple’s AirDrop which works offline. It is important that incidents are reported to the Designated Safeguarding Lead (DSL) or alternates immediately. Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – this is illegal.*

*If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.*

*Do not delete the imagery or ask the young person to delete it.*

*Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).*

*Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.*

*Do not say or do anything to blame or shame any young people involved.*

*Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL*

It is important that all of the above steps are taken as they will provide an evidence trail for the school 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 for dealing with 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:

Students/Pupils Incidents	Actions/Sanctions								
	Refer to safeguarding / online safety lead	Refer to Head of Department/Leader of Learning	Refer to Principal	Report to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning/Detention	Fixed term exclusion/permanent exclusion
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).</b>	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X	X	X	X	X	X	X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X	X	X	X	X	X	X
Unauthorised/inappropriate use of social media/messaging apps/personal email	X	X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	X	X	X	X
Allowing others to access school/academy network by sharing username and passwords	X	X	X	X	X	X	X	X	X
Attempting to access or accessing the school/academy network, using another student's/pupil's account	X	X	X	X	X	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	X	X	X	X
Corrupting or destroying the data of other users	X	X	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	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	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	X	X	X	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	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	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	X	X	X

All outcomes/sanctions above are possible after investigation and severity of the incident has been identified.

## **Appendix**

Appendices

Record of reviewing and logging	34
Social Media Policy	35
School Policy – Online Safety Group Terms of Reference	41
Legislation	44
Glossary of Terms	52
Parent guides	53

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

NB Copleston High school are actively using My Concern for all safeguarding reporting and logging- therefore this will become to tool for reporting and reviewing.

Group:

Date:

Reason for investigation:

Details of first reviewing person

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

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

Web site(s) address/device      Reason for concern

Conclusion and Action proposed or taken

Reporting Log					
Group:					
Date	Time	Incident	Action Taken	Incident Reported By	Signature

Training Needs Audit Log			
Group:			
Relevant training the last 12 months	Identified Training Need	To be met by	Cost
Review Date			

This Policy has been adopted and approved by Gippeswyk Community Educational Trust and has been adapted for use by Copleston High School.

<b>SOCIAL MEDIA POLICY</b>	
Reviewed/Amended	May 2021
Ratified by Copleston LGB	30.6.21
Date of next Review	Summer Term 2022
Responsible Officer	ICT Systems Manager – Charles Greig / DSL – Mr H Palmer / ADSL Mrs Crofton Sleigh
Policy Number	CS8

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

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

### Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

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

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

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

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

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

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

Organisational control

Roles & Responsibilities

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

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

- The aim of the account
- The intended audience
- How the account will be promoted

- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

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

### Monitoring

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

### Behaviour

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

## Legal considerations

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

## Handling abuse

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

## Tone

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

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

## Use of images

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

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

## Personal use

- Staff
- o 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.
- o Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- o Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- o The school permits reasonable and appropriate access to private social media sites.

## Students

- o Staff are not permitted to follow or engage with current or prior students of the school on any personal social media network account.
- o The school's education programme should enable the pupils/students to be safe and responsible users of social media.
- o Students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

## Parents/Carers

- o If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- o The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- o Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

## Monitoring posts about the school

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

## Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private

- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

## Managing school social media accounts

### The Do's

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

### The Don'ts

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

## **School Policy – Online Safety Group Terms of Reference**

### 1. Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. This group is a part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

### 2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include

- SLT member/s
  - Child Protection/Safeguarding officer
  - Teaching staff member
  - Support staff member
  - Online safety coordinator
  - Governor
  - Parent/Carer
  - ICT Technical Support staff (where possible)
  - Community users (where appropriate)
  - Student/pupil representation – for advice and feedback. Student/pupil voice is essential in the make-up of the online safety group, but students/pupils would only be expected to take part in committee meetings where deemed relevant.
- 2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.
- 2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
- 2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature
- 2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

### 3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;

- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

#### 4. Duration of Meetings

Meetings shall be held once a half term. A special or extraordinary meeting may be called when and if deemed necessary.

#### 5. Functions

These are to assist the Online Safety Lead with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school/academy community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
  - Staff meetings/ bulletins
  - Student/pupil forums (for advice and feedback)
  - Governors meetings
  - Surveys/questionnaires for students/pupils, parents/carers and staff
  - Parents evenings
  - Website/VLE/Newsletters
  - Online safety events
  - Internet Safety Day (annually held on the second Tuesday in February)
  - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school/academy
- To monitor filtering/change control logs (e.g. requests for blocking/uN.B.locking sites).
- To monitor the safe use of data across the school/academy
- To monitor incidents involving cyberbullying for staff and pupils

#### 6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for [insert name of organisation] have been agreed

Signed by (SLT):

Date:

Date for review:

Acknowledgement

## **Legislation**

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

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

### Computer Misuse Act 1990

This Act makes it an offence to:

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

School may wish to view the National Crime Agency website which includes information about “Cyber crime – preventing young people from getting involved”. Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

### Data Protection Act 1998

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

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

### The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.

- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

#### Freedom of Information Act 2000

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

#### Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

#### Malicious Communications Act 1988

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

#### Regulation of Investigatory Powers Act 2000

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

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

#### Trade Marks Act 1994

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

#### Copyright, Designs and Patents Act 1988

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

#### Telecommunications Act 1984

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

#### Criminal Justice & Public Order Act 1994

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

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

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

#### Racial and Religious Hatred Act 2006

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

#### Protection from Harassment Act 1997

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

#### Protection of Children Act 1978

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

#### Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

#### Public Order Act 1986

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

#### Obscene Publications Act 1959 and 1964

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

#### Human Rights Act 1998

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

- The right to a fair trial

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

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

#### The Education and Inspections Act 2006

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

#### The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - <http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

#### The Protection of Freedoms Act 2012

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

#### The School Information Regulations 2012

Requires schools to publish certain information on its website:

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

#### Serious Crime Act 2015

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

#### Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

## Links to other organisations or documents

The following links are useful resources alongside online safety policy and matters arising:

UK Safer Internet Centre

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

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

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

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

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

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

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

CEOP

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

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

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

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

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

Netsmartz - <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: [www.360data.org.uk](http://www.360data.org.uk)

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

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

Bullying/Online-bullying/Sexting/Sexual Harassment

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

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

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour -  
<http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/374850/Cyberbullying\\_Advice\\_for\\_Headteachers\\_and\\_School\\_Staff\\_121114.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf)

Childnet – Cyberbullying guidance and practical PSHE toolkit:

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

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

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

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

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

Curriculum

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

UKCCIS – Education for a connected world framework

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.eu/)

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

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

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

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

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

## Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

Parent Guides