



Online Safety Policy

Name of policy	Online Safety
Review committee	SLT
Last review date	September 2024
Next review date	September 2025

Contents

0	Development/Monitoring/Review	of	this	Policy
5	Schedule	for	Development/Monitoring/Review	
5	Scope	of	the	Policy
5	Roles	and		Responsibilities
6	Board	of		Trustees
6	Headteacher	and	Senior	Leaders
6	Online	Safety	Lead	(merged with DSL role)
6	Network		Manager	(external)
7	Teaching	and	Support	Staff
7	Designated	Safeguarding	Lead	(DSL)
7	Online		Safety	Group
				7Students:
				8Parents/Carers
8	Community			Users
8	Policy			Statements
8	Education	-		Students
8	Education	-		Parents/Carers
9	Education	-	The	Wider
9	Education	&	Training	-
10	Training	-	Board	of
10	Technical	-	Infrastructure/Equipment,	Filtering
10	Mobile		Technologies	(including and
11	School-owned/-provided			Monitoring
12	Personal			BYOD/BYOT)
12	Use	of	Digital	devices:
13	Data			devices:
13	The	school	must	Images
13	When	personal	data	is
		is	stored	on
		any	mobile	device
		or	removable	media
		the:		
				14Communications
15	Staff	&	Other	Adults
				15Students
15	Social	Media	-	Protecting
16	When	official	school	social
16	Personal			media
17	Monitoring	of		accounts
17	Dealing	with		are
17	Responding	to		established
19	Illegal			there
20	Other			should
21	School			be:
		Actions		
				Use:
				Media:
				Activities
				Misuse
				Incidents
				Incidents
				Sanctions
				21Appendices
25	Student	Acceptable	Use	Agreement
29	School			Template
29	This	acceptable	use	is
29	Acceptable			intended
29	For	my	own	to
29	I	understand	that	everyone
29	I	will	act	as
30	I	recognise	that	the
		school	has	a
		responsibility	to	maintain
		the	security	and
		integrity	of	the
		technology	it	offers
		me	and	to
		ensure	the	smooth
		running	of	the
		school:		
30	When	using	the	internet
30	I	recognise	that:	
30	I	understand	that	I
30	I	am	responsible	for
30	I	my	actions,	both
30	I	in	and	out
30	I	of	school:	
30	Student	Acceptable	Use	Agreement
31	Student/Pupil	Acceptable	Use	Policy
32	This	is	how	we
		stay	safe	when
		we	use	computers:

32Parent/Carer Acceptable Use Agreement Template
 33This acceptable use policy is intended to ensure:
 33Permission Form
 33Use of Digital/Video Images
 34Digital/Video Images Permission Form
 35Use of Cloud Systems Permission Form
 35Use of Biometric Systems in England and Wales
 36Student Acceptable Use Agreement
 37Staff (and Volunteer) Acceptable Use Policy Agreement Template
 38School Policy
 38This acceptable use policy is intended to ensure:
 38Acceptable Use Policy Agreement
 38For my professional and personal safety:
 38I will be professional in my communications and actions when using school systems:
 39The school and the LA have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
 39When using the internet in my professional capacity or for school sanctioned personal use:
 40I understand that I am responsible for my actions in and out of the school:
 40Acceptable Use Agreement for Community Users Template
 41This acceptable use agreement is intended to ensure:
 41Acceptable Use Agreement
 41Responding to incidents of misuse – flow chart
 42Record of reviewing devices/internet sites (responding to incidents of misuse)
 43Details of first reviewing person
 43Details of second reviewing person
 43Name and location of computer used for review (for websites)
 43Website(s) address/device
 43Reason for concern
 43Conclusion and action proposed or taken
 43Reporting Log
 44Date
 44Time
 44Incident
 44Action Taken
 44Incident Reported By
 44Signature
 44What?
 44By Whom?
 44Training Needs Audit Log
 44Relevant training the last 12 months
 44Identified training need
 44To be met by
 44Cost
 44Review date
 44Legislation
 46Computer Misuse Act 1990
 46Data Protection Act 1998
 46The Data Protection Act 2018:
 46Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:
 46All data subjects have the right to:
 47Freedom of Information Act 2000
 47Communications Act 2003
 47Malicious Communications Act 1988
 47Regulation of Investigatory Powers Act 2000
 47Trade Marks Act 1994
 47Copyright, Designs and Patents Act 1988
 48Telecommunications Act 1984

48Criminal	Justice	&	Public	Order	Act	1994
48Racial	and	Religious		Hatred	Act	2006
48Protection		from	Harassment		Act	1997
48Protection		of	Children		Act	1978
48Sexual		Offences			Act	2003
48Public		Order			Act	1986
49Obscene	Publications		Act	1959	and	1964
49Human		Rights			Act	1998
49The	Education		and	Inspections	Act	2006
49The	Education		and	Inspections	Act	2011
49The	Protection		of	Freedoms	Act	2012
49The	School		Information		Regulations	2012
49Serious		Crime			Act	2015
49Criminal	Justice		and	Courts	Act	2015
50Links	to	other	organisations		or	documents
51UK		Safer		Internet		Centre
						51CEOP
						51Others
51Tools			for			Schools
51Bullying/Online			Bullying/Sexting/Sexual			Harassment
51Social						Networking
						52Curriculum
52Data						Protection
52Professional			Standards/Staff			Training
52Infrastructure/Technical						Support
52Working	with		Parents		and	Carers
						53Prevent
						53Research
53Glossary			of			Terms
						54

Development/Monitoring/Review of this Policy

This online safety policy has been developed by the Senior Leadership Team (SLT).

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

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Trustees Sub Committee on:	27.07.2020
This policy was reviewed by SLT on:	05.11.2024
The implementation of this online safety policy will be monitored by the:	Online Safety Coordinator SLT
Monitoring will take place at regular intervals:	Usually on an annual basis
The Board of Trustees will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Usually on an annual basis
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	November 2025
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Local Authority (LA) Safeguarding Officer, Board of Trustees, 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
 - Staff

Scope of the Policy

This policy applies to all members of the GUST Independent School community (including staff, students, volunteers, parents/carers, visitors, and 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 headteachers 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 are linked to membership of the school. The [2011 Education Act](#) increased these powers with regard to the searching for and of electronic devices and the deletion of data (see Electronic Devices – Searching & Deletion Policy). In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place outside of school.

Roles and Responsibilities

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

Board of Trustees

Trustees 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 Trustees receiving regular information about online safety incidents and monitoring reports. A member of the Trustees has taken on the role of Online Safety Governor (this role has been combined with that of the Child Protection/Safeguarding Governor). The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Lead
- Attendance at Online Safety Group meetings
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Board meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – included in a later section – ‘Responding to incidents of misuse’ and relevant LA disciplinary procedures).
- The Headteacher and senior leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher 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 SLT will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead (merged with DSL role)

- 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's 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 LA/Board of Trustees
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meetings of Governors
- Reports regularly to the SLT

Network Manager (external)

Those with technical responsibilities are responsible for ensuring:

- **The school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **The school meets required online safety technical requirements and any LA online safety policy/guidance that may apply**
- Users may only access networks and devices through a properly enforced password protection policy
- The filtering policy is applied and updated on a regular basis
- 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
- The use of networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher, senior leaders and Online Safety Lead for investigation/action/sanction
- Monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

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 online safety policy and practices**
- **They have read, understood and signed the staff acceptable use policy/agreement (AUP/AUA)**
- **They report any suspected misuse or problem to the Headteacher/senior leaders/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 AUPs
- 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/pupils should be guided to sites checked as suitable for their use and processes should be in place for dealing with any unsuitable material that is found in internet searches

DSL

The 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 online contact with adults/strangers
- Potential or actual incidents of grooming
- Online bullying

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy, including the impact of initiatives.

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

- The production of the school's online safety policy/documents
- 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 students – about the online safety provision
- Monitoring improvement actions identified through the use of the 360-degree safe self-review tool

Students:

- **Are responsible for using the school digital technology systems in accordance with the student/pupil AUA**
- 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 online bullying.
- Should understand the importance of adopting good online safety practices 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' mornings, newsletters, letters, the school 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 practices and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website/learning platform and online student/pupil records
- Their children's personal devices in the school (where this is allowed)

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 systems. ([A community user's AUA template can be found in the appendices.](#))

Policy Statements

Education – Students

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/academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

In planning our online safety curriculum, we will refer to:

- Department for Education (DfE) – Teaching Online Safety in Schools
- Education for a Connected World framework

- SWGfL ProjectEVOLVE – 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:

- Our planned online safety curriculum will be provided as part of Computing/PSHE/other lessons and will be regularly revisited.
- Key online safety messages will be reinforced as part of a planned programme of learner meetings and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of materials/content they access online and be guided to validate the accuracy of information.
- Students 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 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 AUA 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that technical staff (or other relevant designated persons) temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of 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:

- Curriculum activities
- Letters, newsletters, school website, learning platform
- Parent/carer sessions
- High-profile events/campaigns; e.g. Safer Internet Day
- Reference to relevant websites/publications; e.g. www.swgfl.org.uk, www.saferinternet.org.uk/, <http://www.childnet.com/parents-and-carers> (see appendix for further links/resources)

Education – The Wider Community

The school 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 the use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents
- Providing online safety information on the school website for the wider community
- Sharing online safety expertise/good practice with other local schools
- Supporting community groups; e.g. Early Years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision ([possibly supporting the group in the use of Online Compass, an online safety self-review tool for groups such as these – www.onlinecompass.org.uk](#))

Education & Training – Staff/Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. EduCare course on 'Online Safety' written in partnership with Childnet International (<https://www.educare.com/>).
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy and AUAs.
- 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 (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Training – Board of Trustees

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

- Attendance at training provided by the LA/National Governance Association (NGA)/or other relevant organisation (e.g. SWGfL)
- Participation in school training/information sessions for staff or parents

Technical – Infrastructure/Equipment, Filtering and Monitoring

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

[A more detailed technical security template policy can be found in the appendix.](#)

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school 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 Network Manager/Lead Administrator who will keep an up-to-date record of users and their usernames. Users are responsible for

the security of their username and password. (Teachers may choose to use group or class logons and passwords for KS1 and below but should consider whether this models good password practice and need to be aware of the associated risks – see appendix.)

- The ‘administrator’ passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- The Network 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 (see appendix for more details).
- **Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.** N.B. Additional duties for schools 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 (see appendix for information on ‘appropriate filtering’).
- 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 AUA.
- An appropriate system is in place (see flow chart). All incidents of a potentially serious breach will be reported to the DSL and/or Headteacher 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 servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts that might threaten the security of 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 (Acceptable Use Agreement/Mobile Technologies Policy) 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 (Mobile Technologies Policy) that allows staff to/forbids staff from downloading executable files and installing programs 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 BYOD/BYOT)

Mobile technology devices may be school-owned/-provided or personally owned and might include the following: 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 of 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, AUP, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

For further reading, please refer to [NEN Technical Strategy Guidance Note 5 – Bring your own device](#)

- The school's AUAs for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies.
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes			
Internet Only				Yes – secondary	Yes	Yes
No network access				Yes – primary		

School-owned/-provided devices:

- Will be allocated to designated staff on a needs basis – students will be allocated by their teacher
- It would be usual that these can be taken home and used at any appropriate time.
- Staff personal use is allowed outside of work hours and for reasonable actions – students allowed personal use during break times and under guidelines of acceptable use.
- Full network access allowed for all users
- Management of devices/installation of apps/changing of settings/monitoring by Network Manager
- Full network/broadband capacity
- Technical support from Network Manager
- Filtering of devices in line with school
- Access to cloud services available for staff
- Data protection follows policy and guidance
- Taking/storage/use of images follows mobile technologies policy
- Exit processes – if the user leaves the school, the device will be returned and factory reset
- Liability for damage dependent on the reason for damage
- Staff training is not usually necessary – will happen if the staff member needs/requests training

Personal devices:

- All users are allowed personal devices on premises except primary students, who must hand any device in to the Lead Administrator as they enter the school premises.
- Restricted to break times for all users
- Storage
- Staff will usually have access to school devices for school business.
- Levels of access to networks/internet (as above)
- Network/broadband capacity within acceptable use
- No technical support is available.
- Filtering of the internet connection to these devices will be in line with school policy.
- Data protection follows policy and guidance.

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

- The right to take, examine and search users' devices in the case of misuse – this is included in the behaviour policy
- Taking/storage/use of images is strictly forbidden for all users – sanctions are in place for any incidents.
- Disclaimer: school under zero liability for loss/damage or malfunction following access to the network
- Identification/labelling of personal devices is not usually necessary.
- Visitors will be informed about school requirements.
- Education about the safe and responsible use of mobile devices is included in the school online safety Educare 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 – covered as part of the AUA signed by parents/carers at the start of the year.**
- In accordance with guidance from the Information Commissioner's Office (ICO), parents/carers are welcome to take videos and digital images of their children at school 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 in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school 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 individual(s) or the school 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

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

The school must ensure that:

- It has a data protection policy.
- It implements the data protection principles and is able to demonstrate that it does so through the use of policies, notices and records.

- It has paid the appropriate fee to the ICO and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate DPO who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why, and which member of staff has responsibility for managing it.
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- It provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear privacy notice.
- Procedures must be in place to deal with the individual rights of the data subject; e.g. one of the eight data subject rights applicable is that of Subject Access, which enables an individual to see a copy of the personal data held about them (subject to certain exceptions that may apply).
- Data Protection Impact Assessments (DPIAs) are carried out where necessary – for example, to ensure the 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 personal data on the systems. Administrative systems are securely ring-fenced from systems accessible in the classroom/to learners.
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It [reports any relevant breaches to the Information Commissioner](#) within 72 hours of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a freedom of information (FOI) policy that sets out how it will deal with FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

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

- Data must be encrypted and password protected.
- Devices must be password protected.
- Devices must be protected by up-to-date virus and malware-checking software.

- Data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that:

- At all times, they take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- They can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- They can help data subjects understand their rights, know how to handle a request, whether verbal or written, and know who to pass it to in the school
- Where personal data is stored or transferred on mobile or other devices (including USBs), this must be encrypted and password protected
- They will not transfer any school personal data to personal devices except as in line with school policy
- They 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

Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. The following table shows how the school currently considers the benefits of using these technologies for education outweigh their risks/disadvantages:

	Staff & other adults			Students				
	wed	tain mes	l for staff	wed	wed	tain mes	staff sion	wed
Mobile phones may be brought into the school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones/cameras								
Use of other mobile devices; e.g. tablets, gaming devices								
Use of personal email addresses in school or on the school network								
Use of school email for personal emails								

Communication Technologies

Use of messaging apps								
Use of social media								
Use of blogs								

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, virtual learning environment (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.
- Whole-class/group email addresses may be used at KS1, while students at KS2 and above will be provided with individual school email addresses for educational use.
- Students should be taught about online safety issues, such as 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 website, and only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

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

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

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

School staff should ensure that:

- 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 are not attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information

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

- A process for approval by senior leaders

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

Personal Use

- Personal communications are those made via personal social media accounts. In all cases where a personal account is used that associates itself with the school or impacts 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 that do not refer to or impact 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 proactively monitor the internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- The school will use Google Alerts to follow keywords associated with GUST Independent School and staff as part of its reputation alert system.
- The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with school policies.

Dealing with Unsuitable/Inappropriate Activities

Some internet activity – e.g. accessing child abuse images or distributing racist material – is illegal and would obviously be banned from school 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 that 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:

		Acc ept abl e	Acc ept abl e at cer tai n tim es	Acc ept abl e for no mi nat ed use rs	Un acc ept abl e	Un acc ept abl e an d ille gal
User Actions						
Users shall not visit internet sites, make,	Child sexual abuse images – The making, production or distribution of indecent images of children contrary to The Protection of Children Act 1978					X

post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
	Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including the promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information that may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						
<ul style="list-style-type: none"> • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords) • Disabling/impairing/disrupting network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) 						X
	N.B. Schools/academies will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda, the National Crime Agency has a remit to prevent young people from becoming involved in cyber-crime and harness their activity in positive ways.					
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				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 hinder others in their use of the internet)				X	
	Using school systems to run a private business				X	
	Infringing copyright				X	

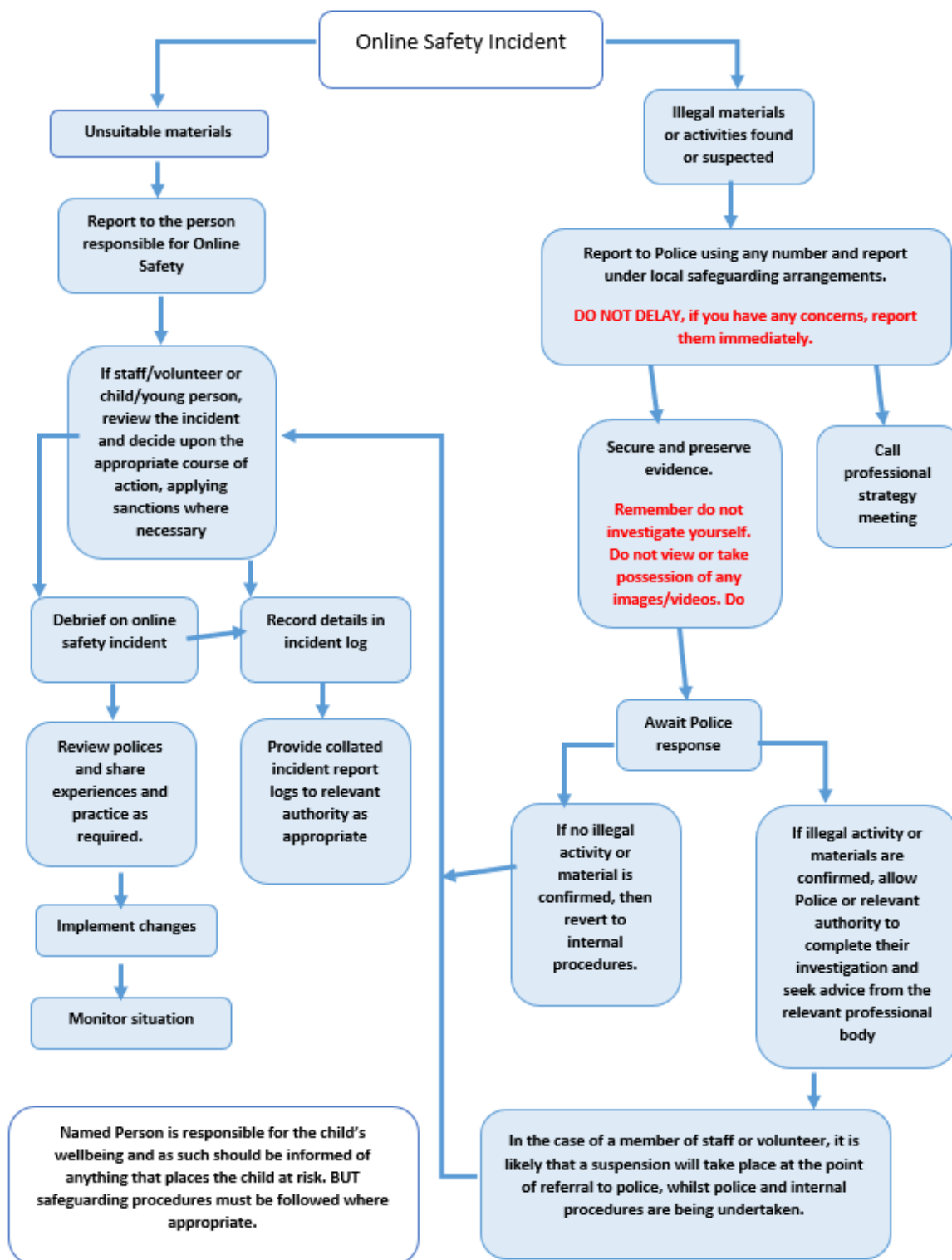
Online gaming (educational)	x				
Online gaming (non-educational)		x			
Online gambling				x	
Online shopping/commerce			x		
File sharing		x			
Use of social media			x		
Use of messaging apps			x		
Use of video broadcasting; e.g. YouTube			x		

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 website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flow chart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school 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, 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 have appropriate internet access to conduct the procedure, but also that 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 LA or national/local organisation (as relevant)
 - Police involvement and/or action
- **If the 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 that potentially breaches the Obscene Publications Act
 - Criminally racist material
 - Promotion of terrorism or extremism
 - Offences under the Computer Misuse Act (see 'User Actions' chart above)
 - Other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

School Actions & Sanctions

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

Actions/Sanctions

	Re fer to cla ss te ac he r	Re fer to Se ni or Le ad er	Re fer to He ad te ac he r	Re fer to Po lic e	Re fer to tec nic al sup port staff for ac tion re fil ter ing /sec urit y, etc.	Inf or m pa re nt s/c ar er s	Re m ov al of ne tw or k/i nt er ne t ac ce ss rig ht s	W ar ning	Further sanctio n; e.g. detenti on/excl usion
Student Incidents									
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		X	X	X		X	X		X
Unauthorised use of non-educational sites during lessons	X	X			X			X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X			X			X	
Unauthorised/inappropriate use of social media/messaging apps/personal email	X	X			X			X	
Unauthorised downloading or uploading of files	X							X	
Allowing others to access the school network by sharing usernames and passwords			X		X	X	X	X	
Attempting to access or accessing the school network, using another student's account		X						X	
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X	X	X	
Corrupting or destroying the data of other users		X	X			X	X	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
Continued infringements of the above, following previous warnings or sanctions			X		X	X	X	X	X
Actions that could bring the school into disrepute or breach the integrity of the ethos of the school			X		X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X	X	X	

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

Actions/Sanctions

Ref er to Se nio r Le ad er	Ref er to He ad ch er	Ref er to LA	Ref er to Pol ice	Refer to Techn ical Suppo rt Staff for action re filterin g, etc.	Wa rni ng	Su sp en sio n	Dis cipl ina ry act ion
---	---	-----------------------	-------------------------------	--	-----------------	----------------------------	--

Staff Incidents

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		X	X	X			X	X
Inappropriate personal use of the internet/social media/personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access the school network by sharing usernames and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X		
Careless use of personal data; e.g. holding or transferring data in an insecure manner	X				X	X		
Deliberate actions to breach data protection or network security rules		X	X				X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X				X

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

Appendices

Contents	Development/Monitoring/Review	of	this	Policy
5	Schedule	for	Development/Monitoring/Review	
5	Scope	of	the	Policy
5	Roles	and		Responsibilities
6	Board	of		Trustees
6	Headteacher	and	Senior	Leaders
6	Online	Safety Lead	(merged with DSL	role)
6	Network		Manager	(external)
7	Teaching	and	Support	Staff
7	Designated	Safeguarding	Lead	(DSL)
7	Online		Safety	Group
				7
				Students:
				8
				Parents/Carers
				Users
8	Community			
8	Policy			Statements
8	Education	-		Students
8	Education	-		Parents/Carers
9	Education	-	The	Wider
9	Education	&	Training	-
10	Training	-	Board	of
10	Technical	-	Infrastructure/Equipment,	Filtering
10	Mobile	Technologies		(including
11	School-owned/-provided			and
12	Personal			Monitoring
12	Use	of	Digital	devices:
12				devices:
12				Images
13	Data			Protection
13	The	school	must	ensure
13	When	personal	data	is
			stored	on
			any	mobile
			device	or
			removable	media
			the:	
				14
				Communications
15	Staff	&	Other	Adults
				15
				Students
15	Social	Media	-	Protecting
16	When	official	school	social
16	Personal			media
17	Monitoring			accounts
17	Dealing	with	Unsuitable/Inappropriate	are
17	Responding	to	Incidents	established
19	Illegal			there
20	Other			should
21	School			be:
				Use:
				Media:
				Activities
				Misuse
				Incidents
				Incidents
				Sanctions
				21
				Appendices
25	Student	Acceptable	Use	Agreement
29	School			Template
29	This	acceptable	use	agreement
29	Acceptable			is
29	For	my	own	personal
29	I	understand	that	everyone
29	I	will	act	as
				I
				expect
				others
				to
				act
				toward
				me:
				30
				I
				recognise
				that:
				30
				I
				am
				responsible
				for
				my
				actions,
				both
				in
				and
				out
				of
				school:
30	Student	Acceptable	Use	Agreement
				Form

31 Student/Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation/KS1)

32 This is how we stay safe when we use computers:

32 Parent/Carer Acceptable Use Agreement Template

33 This acceptable use policy is intended to ensure:

33 Permission Form

33 Use of Digital/Video Images

34 Digital/Video Images Permission Form

35 Use of Cloud Systems Permission Form

35 Use of Biometric Systems in England and Wales

36 Student Acceptable Use Agreement

37 Staff (and Volunteer) Acceptable Use Policy Agreement Template

38 School Policy

38 This acceptable use policy is intended to ensure:

38 Acceptable Use Policy Agreement

38 For my professional and personal safety:

38 I will be professional in my communications and actions when using school systems:

39 The school and the LA have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

39 When using the internet in my professional capacity or for school sanctioned personal use:

40 I understand that I am responsible for my actions in and out of the school:

40 Acceptable Use Agreement for Community Users Template

41 This acceptable use agreement is intended to ensure:

41 Acceptable Use Agreement

41 Responding to incidents of misuse – flow chart

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

43 Details of first reviewing person

43 Details of second reviewing person

43 Name and location of computer used for review (for websites)

43 Website(s) address/device

43 Reason for concern

43 Conclusion and action proposed or taken

43 Reporting Log

44 Date

44 Time

44 Incident Taken

44 Action

44 Incident Reported By

44 Signature

44 What?

44 By Whom?

44 Training Needs Audit Log

44 Relevant training the last 12 months

44 Identified training need

44 To be met by

44 Cost

44 Review date

44 Legislation

46 Computer Misuse Act 1990

46 Data Protection Act 1998

46 The Data Protection Act 2018:

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

46 All data subjects have the right to:

47 Freedom of Information Act 2000

47 Communications Act 2003

47 Malicious Communications Act 1988

47 Regulation of Investigatory Powers Act 2000

47 Trade Marks Act 1994

47	Copyright, Designs and Patents Act	1988
48	Telecommunications Act	1984
48	Criminal Justice & Public Order Act	1994
48	Racial and Religious Hatred Act	2006
48	Protection from Harassment Act	1997
48	Protection of Children Act	1978
48	Sexual Offences Act	2003
48	Public Order Act	1986
49	Obscene Publications Act 1959	1964
49	Human Rights Act	1998
49	The Education and Inspections Act	2006
49	The Education and Inspections Act	2011
49	The Protection of Freedoms Act	2012
49	The School Information Regulations	2012
49	Serious Crime Act	2015
49	Criminal Justice and Courts Act	2015
50	Links to other organisations or documents	
51	UK Safer Internet Centre	
		51CEOP
		51Others
51	Tools for Schools	
51	Bullying/Online Bullying/Sexting/Sexual Harassment	
51	Social Networking	
		52Curriculum
52	Data Protection	
52	Professional Standards/Staff Training	
52	Infrastructure/Technical Support	
52	Working with Parents and Carers	
		53Prevent
		53Research
53	Glossary of Terms	
		54

Student Acceptable Use Agreement (AUA) Template – for secondary students (can be used from KS2 onwards)

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools that open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This AUA is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems in jeopardy. Students/pupils will have good access to digital technologies to enhance their learning, and the school will, in return, expect the *students/pupils* to agree to be responsible users.

AUA

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of 'stranger danger' when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc.).
- If I arrange to meet people offline that I have communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube) unless I have permission from a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices, etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment.
- I understand the risks and will not try to upload, download or access any materials that are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails (unless I know and trust the person/organisation who sent the email) if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).
- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online bullying, use of images or personal information).
- I understand that if I fail to comply with this AUA, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and, in the event of illegal activities, involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the AUA. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Acceptable Use Agreement (AUA) Form

This form relates to the student AUA, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the AUA. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use school systems and devices (both in and out of school)
- I use my own devices in school (when allowed); e.g. mobile phones, gaming devices, USB devices, cameras, etc.
- I use my own equipment out of school in a way that is related to my being a member of this school; e.g. communicating with other members of the school, accessing school email, VLE, website, etc.

Name of Student: _____

Signed: _____

Date: _____

Parent/Carer Countersignature: _____

Student Acceptable Use Agreement (AUA) Template – for younger pupils (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules, I might not be allowed to use a computer/tablet

Signed (child): _____

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age; for younger children, the signature of a parent/carer should be sufficient.)

Signed (parent): _____

Primary schools using this AUA for younger children may also wish to use (or adapt for use) the parent/carer AUA (the template can be found later in the appendix) as this provides additional permission forms (including the digital and video images permission form).

Parent/Carer AUA Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools that open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy (AUP) is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour

The school will try to ensure that *students/pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users. A copy of the *student/pupil* AUA is attached to this permission form so that parents/carers will be aware of the school's expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. ([Schools/academies will need to decide whether or not they wish parents to sign the AUA on behalf of their child.](#))

Permission Form

Parent/Carer Name: _____

Student/Pupil Name: _____

As the parent/carers of the above *students/pupils*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

I know that my son/daughter has signed an AUA and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the AUA with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the AUA.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)
Who will have access to this form
Where this form will be stored
How long this form will be stored for
How this form will be destroyed

Signed: _____

Date: _____

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's **delete as relevant** first name/initials will be used.

The school will comply with the Data Protection Act and request parents'/carers' permission before taking images of members of the school. We will also ensure that when images are published, young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office (ICO), parents/carers are welcome to take videos and digital images of their children at school 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.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form	Where the images may be published, such as Twitter, Facebook, the school website, local press, etc. (see the relevant section of the form below)
Where this form will be stored	Who will have access to the images
How long this form will be stored for	Where the images will be stored

How this form will be destroyed	How long the images will be stored for
	How the images will be destroyed
	How a request for deletion of the images can be made

Digital/Video Images Permission Form

Parent/Carer Name: _____ Student/Pupil Name: _____

As the parent/carers of the above student/pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
<ul style="list-style-type: none"> To support learning activities 	Yes/No
<ul style="list-style-type: none"> In publicity that reasonably celebrates success and promotes the work of the school 	Yes/No
<i>Insert statements here that explicitly detail where images are published by the school.</i>	
I agree that if I take digital or video images at or of school events that include images of children other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: _____

Date: _____

Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for pupils/students.

Schools will need to review and amend the section below, depending on which cloud-hosted services are used.

The school uses **insert cloud service provider name** for *pupils/students* and staff. This permission form describes the tools and pupil/student responsibilities for using these services.

The following services are available to each *pupil/student* as part of the school's online presence in **insert cloud service provider name**:

Using **insert cloud service provider name** will enable your child to collaboratively create, edit and share files and websites for school-related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that the use of the tools significantly adds to your child's educational experience.

As the school is collecting personal data and sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form	What data will be shared
Where this form will be stored	Who the data will be shared with
How long this form will be stored for	Who will have access to the data
How this form will be destroyed	Where the data will be stored

	How long the data will be stored for
	How the data will be destroyed
	How a request for deletion of the data can be made

Do you consent to your child having access to this service? Yes/No

Student/Pupil Name: _____ Parent/Carer Name: _____

Signed: _____ Date: _____

Use of Biometric Systems in England and Wales

If the school uses biometric systems (e.g. fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending, etc. it must (under the 'Protection of Freedoms' and data protection legislation) seek permission from a parent or carer.

The school uses biometric systems for the recognition of individual children in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library), so nothing can be lost, such as a swipe card.

The school has carried out a data privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints/palms are stored, and the original image cannot be reconstructed from the data. This means that it is not possible, for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is, in effect, a string of numbers.

As the school is collecting special-category personal data and **delete as appropriate** sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form	What data will be shared
Where this form will be stored	Who the data will be shared with
How long this form will be stored for	Who will have access to the data
How this form will be destroyed	Where the data will be stored
	How long the data will be stored for
	How the data will be destroyed
	How consent to process the biometric data can be withdrawn

Parent/Carer Name: _____

Student/Pupil Name: _____

As the parent/carer of the above student/pupil, I agree to the school using biometric recognition systems, as described above. Yes/No

I understand that the images cannot be used to create a whole [fingerprint/palm print](#) of my child and that these images will not be shared with anyone outside the school. Yes/No

Signed: _____

Further guidance

- Each parent of the child should be notified by the school that they are planning to process their child's biometrics and that they are able to object.
- In order for a school to process children's biometrics, at least one parent must consent, and no parent has withdrawn consent. This needs to be in writing.
- The child can object or refuse to participate in the processing of their biometric data regardless of parents' consent.
- Schools and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.
- Permission only needs to be collected once during the period that the student/pupil attends the school, but new permission is required if there are changes to the biometric systems in use.

Student Acceptable Use Agreement (AUA)

On the following pages, we have copied, for the information of parents and carers, the student AUA.

It is suggested that when the student/pupil AUA is written, a copy should be attached to the parent/carer AUA to provide information for parents and carers about rules and behaviours that students/pupils have committed to by signing the form.

Staff (and Volunteer) Acceptable Use Policy (AUP) Agreement Template

Sections that include advice or guidance are written in **BLUE**. It is anticipated that schools/academies will remove these sections from their final document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their online safety policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final AUP will be more concise.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools that open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This AUP is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That staff are protected from potential risk in their use of technology in their everyday work

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work and enhance learning opportunities for *students/pupils'* learning and will, in return, expect staff and volunteers to agree to be responsible users.

AUP Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school's digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to the use of these technologies (e.g. laptops, email, VLE, etc.) out of school and to the transfer of personal data (digital or paper-based) out of school. (Schools/academies should amend this section in the light of their policies that relate to the use of school systems and equipment out of school.)
- I understand that the school's digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (Schools should amend this section in the light of their policies that relate to the personal use, by staff and volunteers, of school systems.)

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others, I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the school website/VLE), it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies. [\(Schools/academies should amend this section to take account of their policy on access to social networking and similar sites.\)](#)
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. [\(Schools should amend this section to take account of their policy on communications with students/pupils and parents/carers. Staff should be made aware of the risks attached to using their personal email addresses/mobile phones/social networking sites for such communications.\)](#)
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the LA have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses. [\(Schools/academies should amend this section in light of their policies that relate to the use of staff devices.\)](#)
- I will not use personal email addresses on school ICT systems. [\(Schools/academies should amend this section in light of their email policy – some schools/academies will choose to allow the use of staff personal email addresses on the premises.\)](#)
- I will not open any hyperlinks in emails or any attachments to emails unless the source is known and trusted or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials that are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine or store programs on a computer, nor will I try to alter computer settings unless this is allowed in school policies. [\(Schools/academies should amend this section in light of their policies on installing programs/altering settings.\)](#)
- I will not disable or cause any damage to school equipment or equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school/LA personal data policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software however this may have happened.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this AUP applies not only to my work and use of school digital technology equipment in school but also to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this AUA, I could be subject to disciplinary action. This could include [\(schools/academies should amend this section to provide relevant sanctions as per their behaviour policies\)](#) a warning, a suspension, referral to governors/directors and/or the LA, and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____

Acceptable Use Agreement (AUA) for Community Users Template

This AUA is intended to ensure:

- That community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- That school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That users are protected from potential harm in their use of these systems and devices

AUA

I understand that I must use school systems and devices in a responsible way to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials that are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files without permission.
- I will ensure that if I take and/or publish images of others, I will only do so with their permission. I will not use my personal equipment to record these images without permission. If images are published, it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a school device, nor will I try to alter computer settings unless I have permission to do so.
- I will not disable or cause any damage to school equipment or equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this AUA, the school has the right to remove my access to school systems/devices.

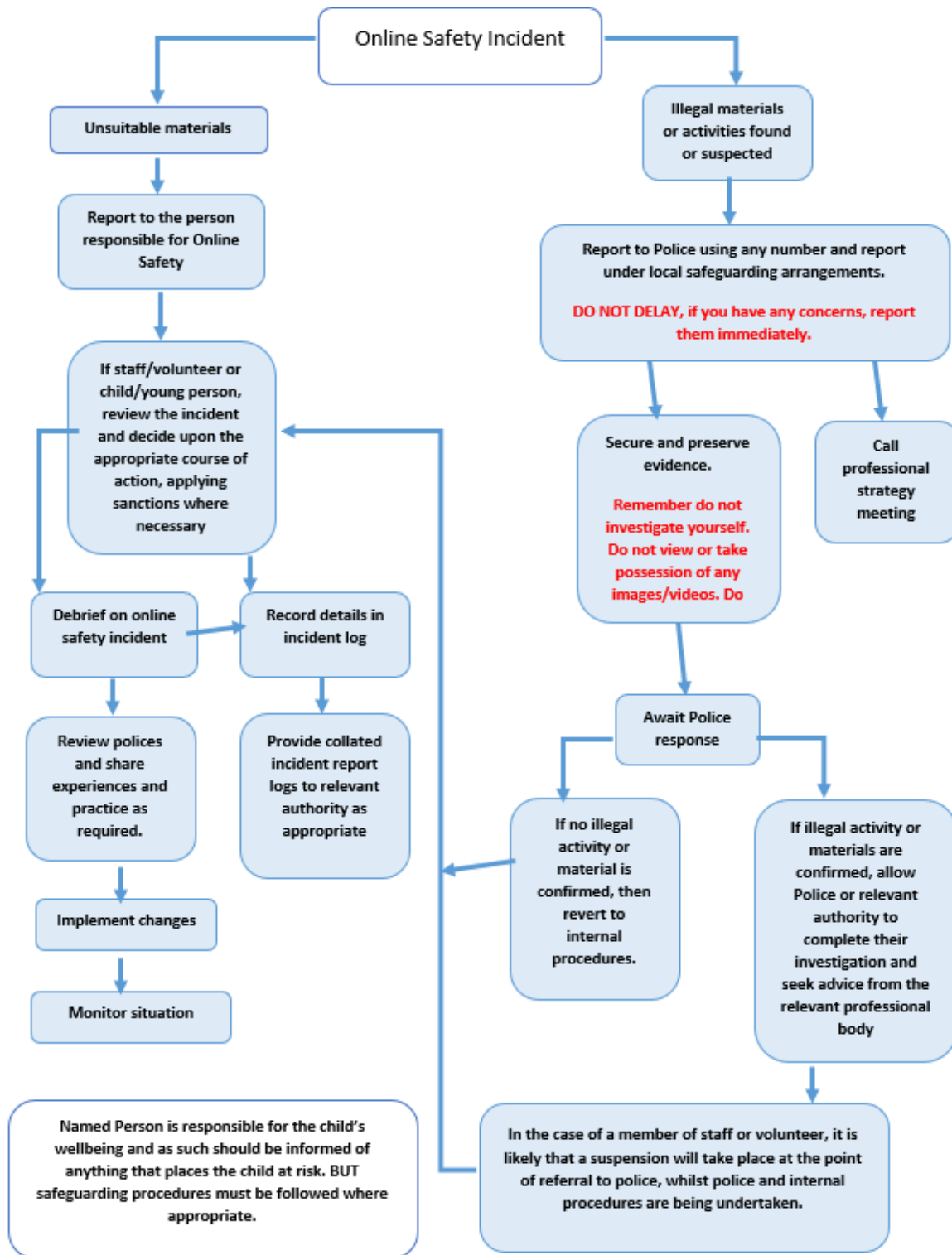
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

As the school is collecting personal data by issuing this form, it should inform community users about:

Who will have access to this form	How this form will be destroyed
Where this form will be stored	How long this form will be stored for

Name: _____ Signed: _____ Date: _____

Responding to incidents of misuse – flow chart



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

Group: _____

Date: _____

Reason for investigation: _____

Details of first reviewing person

Name: _____

Position: _____

Signature: _____

Details of second reviewing person

Name: _____

Position: _____

Signature: _____

Name and location of computer used for review (for websites)

Website(s) address/device	Reason for concern

Conclusion and action proposed or taken

Reporting Log

Group: _____

Date	Time	Incident	Action Taken	
			What?	By Whom?

Training Needs Audit Log

Group: _____

Relevant training in the last 12 months	Identified training need	To be met by

Legislation

Schools/academies 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

Schools/academies 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 individuals' 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 personal 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 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 another 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 that 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 helpline 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) 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 copyrighted work. There are, however, certain limited user permissions, such as fair dealing, which means in 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, 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 that 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 that 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 that amounts to harassment of another and that they know 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 them is guilty of an offence if they know or ought to know that their 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, and Connexions staff fall into 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 that is threatening. As per 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 that 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 gives 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 a new offence of sexual communication with a child. Also created new offences and orders around gang crime (including child sexual exploitation (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 may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

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

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

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

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

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

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

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

CEOP

CEOP – <http://ceop.police.uk/>

Think U Know – <https://www.thinkuknow.co.uk/>

Others

LGfL – [Online Safety Resources](#)

Kent – [Online Safety Resources page](#)

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

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

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

Tools for Schools

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

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

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

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

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

Bullying/Online Bullying/Sexting/Sexual Harassment

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

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

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

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

DfE – Cyberbullying guidance –

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit –

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

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

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

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC – [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Curriculum

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

[UKCCIS – Education for a connected world framework](#)

Teach Today – www.teachtoday.eu/

Insafe – [Education Resources](#)

Data Protection

[360data free questionnaire and data protection self review tool](#)

[ICO Guides for Education \(wide range of sector specific guides\)](#)

[DfE advice on Cloud software services and the Data Protection Act](#)

[IRMS – Records Management Toolkit for Schools](#)

[NHS – Caldicott Principles \(information that must be released\)](#)

[ICO Guidance on taking photos in schools](#)

[Dotkumo – Best practice guide to using photos](#)

Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

[DfE – Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset – [Questions for Technical Support](#)

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

Working with Parents and Carers

[Online Safety BOOST Presentations – parent’s presentation](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online – resources for parents](#)

[Teach Today – resources for parents’ workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

[NCA – Cyber Prevent](#)

Childnet – [Trust Me](#)

Research

[Ofcom – Media Literacy Research](#)

Further links can be found at the end of the UKCIS [Education for a Connected World framework](#).

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of the 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 Commissioner’s 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 regional broadband consortia (e.g. SWGfL) to provide 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 LAs – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU-funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting)
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World framework](#).

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

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