THE APPLETON SCHOOL

Online Safety Policy

Adopted by the Governing Body ........................................ Date

Signature Chair of Governors ............................................

April 2020
## Contents

- Development/Monitoring/Review of this Policy 3
- Roles and Responsibilities 4
- Policy Statements 7
- Communications 13
- Dealing with unsuitable/inappropriate activities 15
- Responding to incidents of misuse 16
- Illegal Incidents 17
- Other Incidents 18
- School/academy actions & sanctions 19
- Appendices 22
  - Student/Pupil Acceptable Use Agreement Template – for older students/pupils 23
  - Parent/Carer Acceptable Use Agreement Template 25
  - Staff (and Volunteer) Acceptable Use Policy Agreement Template 29
- Responding to incidents of misuse – flow chart 31
- Record of reviewing devices/internet sites (responding to incidents of misuse) 32
- Reporting Log 33
- Training Needs Audit Log 34
- Legislation 35
- Glossary of Terms 41
Development/Monitoring/Review of this Policy

This online safety policy will be developed by a working group Online Safety at The Appleton School made up of:

- Headteacher and senior leaders
- School Designated Safeguarding Lead
- Online Safety Officer/Coordinator
- Staff – including teachers, support staff, technical staff
- Governors
- Parents and carers

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

Schedule for Development/Monitoring/Review

<table>
<thead>
<tr>
<th>Schedule for Development/Monitoring/Review</th>
<th>Insert date</th>
</tr>
</thead>
<tbody>
<tr>
<td>This online safety policy was approved by the Governing Body/Governors Sub Committee on:</td>
<td>Insert date</td>
</tr>
<tr>
<td>The implementation of this online safety policy will be monitored by the:</td>
<td>Online Safety Coordinator, Group,</td>
</tr>
<tr>
<td>Senior Leadership Team</td>
<td></td>
</tr>
<tr>
<td>Monitoring will take place at regular intervals:</td>
<td>Yearly</td>
</tr>
<tr>
<td>The Governing Body/Governors Sub Committee will receive a report on the implementation of the online safety</td>
<td>Twice a year</td>
</tr>
<tr>
<td>policy generated by the monitoring group (which will include anonymous details of online safety incidents)</td>
<td></td>
</tr>
<tr>
<td>at regular intervals:</td>
<td></td>
</tr>
<tr>
<td>The online safety policy will be reviewed annually, or more regularly in the light of any significant new</td>
<td>September 2020</td>
</tr>
<tr>
<td>developments in the use of the technologies, new threats to online safety or incidents that have taken place.</td>
<td></td>
</tr>
<tr>
<td>The next anticipated review date will be:</td>
<td></td>
</tr>
<tr>
<td>Should serious online safety incidents take place, the following external persons/agencies should be</td>
<td>LA Safeguarding Officer, Academy</td>
</tr>
<tr>
<td>informed:</td>
<td>Group Officials, LADO, Police</td>
</tr>
<tr>
<td>The school will monitor the impact of the policy using:</td>
<td></td>
</tr>
<tr>
<td>- Logs of reported incidents - CPOMS</td>
<td></td>
</tr>
<tr>
<td>- Monitoring logs of internet activity (including sites visited)/filtering - Smoothwall</td>
<td></td>
</tr>
<tr>
<td>- Internal monitoring data for network activity - Smoothwall</td>
<td></td>
</tr>
<tr>
<td>- Surveys/questionnaires of</td>
<td></td>
</tr>
<tr>
<td>o students/pupils</td>
<td></td>
</tr>
<tr>
<td>o parents/carers</td>
<td></td>
</tr>
<tr>
<td>o staff</td>
<td></td>
</tr>
</tbody>
</table>

Scope of the Policy

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

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

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

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

Governors/Board of Directors

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

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

Headteacher/Principal 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 Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority 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 Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authorityrelevant body
- 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 Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

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

Teaching and Support Staff
Are responsible for ensuring that:

• they have an up to date awareness of online safety matters and of the current school 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 Leader/Online Safety Lead for investigation/action/sanction
• all digital communications with students/pupilsgetParents/carers should be on a professional level and only carried out using official school systems
• online safety issues are embedded in all aspects of the curriculum and other activities
• students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
• in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

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

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

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

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

• the production/review/monitoring of the school online safety policy/documents.
• the production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
• mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
• monitoring network/internet/filtering/incident logs
• consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
• monitoring improvement actions identified through use of the 360 degree safe self-review tool
**Students/Pupils:**
- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

**Parents/carers**
Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
- digital and video images taken at school events
- access to parents’ sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)

**Community Users**
Community Users who access school/academy 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.
Policy Statements

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

When planning The Appleton School online safety curriculum reference has been made to the following resources:
- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
- A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and are regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are 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.
- Students are helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff 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 are 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 are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/carers
Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children’s online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:
- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers
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 use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision e.g. www.onlinecompass.org.uk

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

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

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.
- 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:

- School technical systems will be managed in ways that ensure that the school/academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the school Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master/administrator” passwords for the school/academy systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school/academy safe)
• The school 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

• Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

• Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

• The school has provided enhanced/differentiated user-level filtering

• School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.

• An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).

• Appropriate security measures are in place (schools/academies may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.

• An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

• An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.

• An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.

• An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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

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

• The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies

• The school allows:
<table>
<thead>
<tr>
<th></th>
<th>School Devices</th>
<th>Personal Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>School owned for</strong></td>
<td><strong>Authorised</strong></td>
<td><strong>School owned</strong></td>
</tr>
<tr>
<td><strong>single user</strong></td>
<td>device¹</td>
<td>for multiple</td>
</tr>
<tr>
<td></td>
<td></td>
<td>users</td>
</tr>
<tr>
<td><strong>Allowed in school</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Full network access</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Internet only</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>No network access</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **School owned**       | **Staff owned** |
| **for multiple users** |                |
| **Allowed in school**  | Yes/No²        |
| **Full network access**| Yes/No²        |
| **Internet only**      | Yes/No²        |
| **No network access**  | Yes/No²        |

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

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

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

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.
² The school should add below any specific requirements about the use of mobile/personal devices in school.
Use of digital and video images
The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student’s work can only be published with the permission of the student and parents or carers.

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

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. (see appendix for template policy)
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner’s Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school/academy may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- it has an ‘information asset register’ in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
• it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a “retention policy” to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.

• it provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix).

• procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).

• data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)

• IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

• it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.

• it understands how to share data lawfully and safely with other relevant data controllers.

• it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.

• If a maintained school/academy, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.

• all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual’s rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:
• data must be encrypted and password protected.
• device must be password protected.
• device must be protected by up to date virus and malware checking software
• data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.

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

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

<table>
<thead>
<tr>
<th>Communication Technologies</th>
<th>Staff &amp; other adults</th>
<th>Students/Pupils</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile phones may be brought to the school/academy</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Use of mobile phones in lessons</td>
<td>Allowed at certain times</td>
<td>Allowed at certain times</td>
</tr>
<tr>
<td>Use of mobile phones in social time</td>
<td>Allowed for selected staff</td>
<td>Allowed with staff permission</td>
</tr>
<tr>
<td>Taking photos on mobile phones/cameras</td>
<td>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Use of other mobile devices e.g. tablets, gaming devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of personal email addresses in school/academy, or on school/academy network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of school/academy email for personal emails</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of messaging apps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of social media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of blogs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In addition to the table above, the school also has the following policy statements about the use of communications technologies:

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/pupils 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/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students at KS2 and above will be provided with individual school/academy email addresses for educational use.
Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

When managing risk and behaviour online the core message is the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers’ professional conduct are set out in ‘Teachers Standards 2012’. Ofsted’s online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority 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 risk of harm to pupils, staff and the school through:

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

School staff should ensure that:

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

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

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

Personal Use:

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

Monitoring of Public Social Media:

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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.
**Dealing with unsuitable/inappropriate activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school/academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

### User Actions

<table>
<thead>
<tr>
<th>Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</th>
<th>Acceptable</th>
<th>Acceptable at certain times</th>
<th>Acceptable for nominated users</th>
<th>Unacceptable</th>
<th>Unacceptable and illegal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Pornography</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Promotion of any kind of discrimination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Threatening behaviour, including promotion of physical violence or mental harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Promotion of extremism or terrorism</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

### Activities that might be classed as cyber-crime under the Computer Misuse Act:
- Gaining unauthorised access to school networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)

15
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

<table>
<thead>
<tr>
<th>Activity</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school</td>
<td>X</td>
</tr>
<tr>
<td>Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)</td>
<td>X</td>
</tr>
<tr>
<td>Unfair usage (downloading/uploading large files that hinders others in their use of the internet)</td>
<td>X</td>
</tr>
<tr>
<td>Using school systems to run a private business</td>
<td>X</td>
</tr>
<tr>
<td>Infringing copyright</td>
<td>X</td>
</tr>
<tr>
<td>On-line gaming (educational)</td>
<td></td>
</tr>
<tr>
<td>On-line gaming (non-educational)</td>
<td></td>
</tr>
<tr>
<td>On-line gambling</td>
<td></td>
</tr>
<tr>
<td>On-line shopping/commerce</td>
<td></td>
</tr>
<tr>
<td>File sharing</td>
<td></td>
</tr>
<tr>
<td>Use of social media</td>
<td></td>
</tr>
<tr>
<td>Use of messaging apps</td>
<td></td>
</tr>
<tr>
<td>Use of video broadcasting e.g. Youtube</td>
<td></td>
</tr>
</tbody>
</table>

**Responding to incidents of misuse**

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).
Illegal Incidents

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

Named Person is responsible for the child’s wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
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, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority Group or national/local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - Incidents of ‘grooming’ behaviour
  - The sending of obscene materials to a child
  - Adult material which potentially breaches the Obscene Publications Act
  - Criminal 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:

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

<table>
<thead>
<tr>
<th>Staff Incidents</th>
<th>Actions/Sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).</td>
<td>X X X</td>
</tr>
<tr>
<td>Inappropriate personal use of the internet/social media/personal email</td>
<td></td>
</tr>
<tr>
<td>Unauthorised downloading or uploading of files</td>
<td></td>
</tr>
<tr>
<td>Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account</td>
<td></td>
</tr>
<tr>
<td>Careless use of personal data e.g. holding or transferring data in an insecure manner</td>
<td></td>
</tr>
<tr>
<td>Deliberate actions to breach data protection or network security rules</td>
<td></td>
</tr>
<tr>
<td>Corrupting or destroying the data of other users or causing deliberate damage to hardware or software</td>
<td></td>
</tr>
<tr>
<td>Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature</td>
<td></td>
</tr>
<tr>
<td>Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils</td>
<td></td>
</tr>
<tr>
<td>Actions which could compromise the staff member’s professional standing</td>
<td></td>
</tr>
<tr>
<td>Actions which could bring the school into disrepute or breach the integrity of the ethos of the school/academy</td>
<td></td>
</tr>
<tr>
<td>Using proxy sites or other means to subvert the school’s filtering system</td>
<td></td>
</tr>
<tr>
<td>Accidentally accessing offensive or pornographic material and failing to report the incident</td>
<td></td>
</tr>
<tr>
<td>Deliberately accessing or trying to access offensive or pornographic material</td>
<td></td>
</tr>
<tr>
<td>Breaching copyright or licensing regulations</td>
<td></td>
</tr>
<tr>
<td>Continued infringements of the above, following previous warnings or sanctions</td>
<td></td>
</tr>
</tbody>
</table>
Appendices

Student/Pupil Acceptable Use Agreement Template – for older students/pupils .......................................................... 23

Student/Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation/KS1) Error! Bookmark not defined.

Parent/Carer Acceptable Use Agreement Template ........................................................................................................... 25

Staff (and Volunteer) Acceptable Use Policy Agreement Template .......................................................................................... 29

Acceptable Use Agreement for Community Users Template ................................................................. Error! Bookmark not defined.

Responding to incidents of misuse – flow chart ................................................................................................................. 31

Record of reviewing devices/internet sites (responding to incidents of misuse) ......................................................... 32

Reporting Log ....................................................................................................................................................... 33

Training Needs Audit Log ............................................................................................................................................. 34

School Technical Security Policy Template (including filtering and passwords) Error! Bookmark not defined.

School/academy Personal Data Advice and Guidance ............................................................... Error! Bookmark not defined.

School/academy policy template: Electronic Devices - Searching & Deletion Error! Bookmark not defined.

Mobile Technologies Policy Template (inc. BYOD/BYOT) ........................................................ Error! Bookmark not defined.

Social Media Policy Template ............................................................................................................................... Error! Bookmark not defined.

School Policy Template – Online Safety Group Terms of Reference .......... Error! Bookmark not defined.

Legislation........................................................................................................................................................................... 35

Glossary of Terms.......................................................................................................................................................
Student/Pupil Acceptable Use Agreement

School/academy 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, which 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 acceptable use agreement 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 and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use 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.

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 on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, 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 on-line.

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 the school/academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of 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 was using school equipment.
• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes 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, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
• I will not install or attempt to install or store programmes 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 the 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 acceptable use agreement, 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 acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

**Student Acceptable Use Agreement Form**
This form relates to the student acceptable use agreement; 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 acceptable use agreement. 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 the school systems and devices (both in and out of school).
• I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
• I use my own equipment out of the school/academy in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student: 

Group/Class: 

Signed: 

Date: 

Parent/Carer countersignature: 

24
Parent/Carer Acceptable Use Agreement 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, which 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 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/academy 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 will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the student acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school 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.

Permission Form

Parent/Carers Name: .............................................................................................................

Student Name: ......................................................................................................................

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

I know that my son/daughter has signed an acceptable use agreement 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.

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/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 acceptable use agreement.

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.

<table>
<thead>
<tr>
<th>Printed &amp; electronic</th>
<th>Data team</th>
<th>Electronically under student profile/documents</th>
<th>7 years after date of leaving</th>
<th>Shredded/deleted</th>
</tr>
</thead>
</table>
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 first name initials will be used.

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

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

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

<table>
<thead>
<tr>
<th>This form (electronic or printed)</th>
<th>The images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who will have access to this form.</td>
<td>Where the images may be published. Such as; Twitter, Facebook, the school/academy website, local press, etc. (see relevant section of form below)</td>
</tr>
<tr>
<td>Where this form will be stored.</td>
<td>Who will have access to the images.</td>
</tr>
<tr>
<td>How long this form will be stored for.</td>
<td>Where the images will be stored.</td>
</tr>
<tr>
<td>How this form will be destroyed.</td>
<td>How long the images will be stored for.</td>
</tr>
<tr>
<td></td>
<td>How the images will be destroyed.</td>
</tr>
<tr>
<td></td>
<td>How a request for deletion of the images can be made.</td>
</tr>
</tbody>
</table>

Digital/Video Images Permission Form
Parent/Carers Name: .................................................. Student Name: ..................................................

As the parent/carer 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:

• to support learning activities. Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.

Insert statements here that explicitly detail where images are published by the school/academy

I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

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 use of the tools significantly adds to your child’s educational experience.

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

<table>
<thead>
<tr>
<th>This form (electronic or printed)</th>
<th>The data shared with the service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who will have access to this form.</td>
<td>Who the data will be shared with</td>
</tr>
<tr>
<td>Where this form will be stored.</td>
<td>Where the data will be stored.</td>
</tr>
<tr>
<td>How long this form will be stored for.</td>
<td>Where the data will be stored.</td>
</tr>
<tr>
<td>How this form will be destroyed.</td>
<td>How long the data will be stored for.</td>
</tr>
<tr>
<td></td>
<td>How the data will be destroyed.</td>
</tr>
<tr>
<td></td>
<td>How a request for deletion of the data can be made.</td>
</tr>
</tbody>
</table>

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

Student Name: ............................................. Parent/Carers Name: .............................................

Signed: ............................................. Date: .............................................

Use of Biometric Systems in England and Wales

The school uses biometric systems for the recognition of individual children in the following ways.

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them 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 are stored and the original image cannot be reconstructed from the data. Meaning 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 sharing this with a third party, it should inform parents/carers about:

<table>
<thead>
<tr>
<th>This form (electronic or printed)</th>
<th>The data shared with the service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who will have access to this form.</td>
<td>What data will be shared</td>
</tr>
<tr>
<td>Where this form will be stored.</td>
<td>Who the data will be shared with</td>
</tr>
<tr>
<td>How long this form will be stored for.</td>
<td>Who will have access to the data.</td>
</tr>
<tr>
<td>How this form will be destroyed.</td>
<td>Where the data will be stored.</td>
</tr>
<tr>
<td></td>
<td>How long the data will be stored for.</td>
</tr>
<tr>
<td></td>
<td>How the data will be destroyed.</td>
</tr>
<tr>
<td></td>
<td>How consent to process the biometric data can be withdrawn.</td>
</tr>
</tbody>
</table>

Parent/Carers Name: ..........................................................  
Student Name: .................................................................

As the parent/carer of the above student/pupil, I agree to the school using biometric recognition systems, as described above.  

I understand that the images cannot be used to create a whole fingerprint of my child and that these images will not be shared with anyone outside the school.  

Signed: .................................................................

Further guidance

- Each parent of the child should be notified by the school/academy that they are planning to process their child's biometrics and notified 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 attends the school, but new permission is required if there are changes to the biometric systems in use.

**Student/Pupil Acceptable Use Agreement**

On the following pages we have copied, for the information of parents and carers, the student/pupil acceptable use agreement.
Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy
New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which 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 acceptable use policy 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, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy 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 digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to 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.
- I understand that the school 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.
- 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.
I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

I will not engage in any on-line activity that may compromise my professional responsibilities.

**The school and the local authority 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 was 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.
- I will not use personal email addresses on the school/academy ICT systems.
- 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 programmes).
- 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 which 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 programmes or software that might allow me to bypass the 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 programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school/academy policies.
- I will not disable or cause any damage to school/academy equipment, or the 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/academy 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 acceptable use policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/academy 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 acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority 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: ..........................................................
Responding to incidents of misuse – flow chart

Online Safety Incident

- Unsuitable materials:
  - Report to the person responsible for Online Safety

- If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
  - Debrief on online safety incident
  - Review policies and share experiences and practice as required.
  - Implement changes
  - Monitor situation

- Illegal materials or activities found or suspected:
  - Record details in incident log
  - Provide collated incident report logs to relevant authority as appropriate
  - Monitor situation

- Report to Police using any number and report under local safeguarding arrangements.
  - Secure and preserve evidence.
    - Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
      - Call professional strategy meeting
  - Wait Police response
    - If no illegal activity or material is confirmed, then revert to internal procedures.
    - In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

- Named Person is responsible for the child’s wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .................................................................
Date: ........................................................................
Reason for investigation: .................................................................
........................................................................
Details of first reviewing person
Name: ........................................................................
Position: .................................................................
Signature: ........................................................................

Details of second reviewing person
Name: ........................................................................
Position: .................................................................
Signature: ........................................................................

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

<table>
<thead>
<tr>
<th>Web site(s) address/device</th>
<th>Reason for concern</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conclusion and Action proposed or taken
........................................................................
........................................................................
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Incident</th>
<th>Action Taken</th>
<th>Incident Reported By</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Training Needs Audit Log

**Group:** .................................................................

<table>
<thead>
<tr>
<th>Relevant training the last 12 months</th>
<th>Identified Training Need</th>
<th>To be met by</th>
<th>Cost</th>
<th>Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Legislation

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

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

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

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

The Data Protection Act 2018:

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

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

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.
**Freedom of Information Act 2000**
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

**Communications Act 2003**
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Malicious Communications Act 1988**
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

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

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

**Trade Marks Act 1994**
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

**Copyright, Designs and Patents Act 1988**
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

**Telecommunications Act 1984**
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

**Criminal Justice & Public Order Act 1994**
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.
Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

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

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

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.
(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

**The Protection of Freedoms Act 2012**
Requires schools to seek permission from a parent/carer to use Biometric systems

**The School Information Regulations 2012**
Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

**Serious Crime Act 2015**
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

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

For further guidance or support please contact the Revenge Porn Helpline

**Links to other organisations or documents**
The following links 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/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/

**CEOP**
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

**Others**
LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety
Netsmartz - http://www.netsmartz.org/

**Tools for Schools**
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
**Bullying/Online-bullying/Sexting/Sexual Harassment**

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

SELMA – Hacking Hate - [https://selma.swgfl.co.uk](https://selma.swgfl.co.uk)


Scottish Government - Better relationships, better learning, better behaviour - [http://www.scotland.gov.uk/Publications/2013/03/7388](http://www.scotland.gov.uk/Publications/2013/03/7388)


Childnet – Project deSHAME – Online Sexual Harassment

UKSIC – Sexting Resources

Anti-Bullying Network – [http://www.antibullying.net/cyberbullying1.htm](http://www.antibullying.net/cyberbullying1.htm)

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

**Social Networking**

Digizen – [Social Networking](http://www.antibullying.net/cyberbullying1.htm)

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](https://projectevolve.co.uk)

UKCCIS – Education for a connected world framework

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

In safe - [Education Resources](http://enable.eun.org/)

**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](https://selma.swgfl.co.uk)

NCA – [Guide to the Computer Misuse Act](http://www.scotland.gov.uk/Publications/2013/03/7388)

NEN – [Advice and Guidance Notes](http://www.scotland.gov.uk/Publications/2013/03/7388)
Working with parents and carers
Online Safety BOOST Presentations - parent’s presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent
Prevent Duty Guidance
Prevent for schools – teaching resources
NCA – Cyber Prevent
Childnet – Trust Me

Research
Ofcom – Media Literacy Research

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

**AUP/AUA**  Acceptable Use Policy/Agreement – see templates earlier in this document

**CEOP**  Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

**CPD**  Continuous Professional Development

**FOSI**  Family Online Safety Institute

**ICO**  Information Commissioners Office

**ICT**  Information and Communications Technology

**INSET**  In Service Education and Training

**IP address**  The label that identifies each computer to other computers using the IP (internet protocol)

**ISP**  Internet Service Provider

**ISPA**  Internet Service Providers’ Association

**IWF**  Internet Watch Foundation

**LA**  Local Authority

**LAN**  Local Area Network

**MIS**  Management Information System

**NEN**  National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

**Ofcom**  Office of Communications (Independent communications sector regulator)

**SWGfL**  South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

**TUK**  Think U Know – educational online safety programmes for schools, young people and parents.

**UKSIC**  UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

**UKCIS**  UK Council for Internet Safety

**VLE**  Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.

**WAP**  Wireless Application Protocol