Online Policy

Adopted by the Governing Body on 22.11.2022

November 2022
# Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development/Monitoring/Review of this Policy</td>
<td>3</td>
</tr>
<tr>
<td>Aims</td>
<td>3</td>
</tr>
<tr>
<td>Legislation and guidance</td>
<td>4</td>
</tr>
<tr>
<td>Roles and Responsibilities</td>
<td>9</td>
</tr>
<tr>
<td>Policy Statements (including education)</td>
<td>13</td>
</tr>
<tr>
<td>Communications</td>
<td>19</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td>21</td>
</tr>
<tr>
<td>Acceptable use of the internet in school</td>
<td>22</td>
</tr>
<tr>
<td>Pupils using mobile devices in school</td>
<td>22</td>
</tr>
<tr>
<td>Staff using work devices outside school</td>
<td>23</td>
</tr>
<tr>
<td>How the school will respond to issues of misuse</td>
<td>23</td>
</tr>
<tr>
<td>Training</td>
<td>30</td>
</tr>
<tr>
<td>Monitoring arrangements</td>
<td>31</td>
</tr>
<tr>
<td>Links with other policies</td>
<td>31</td>
</tr>
</tbody>
</table>

## Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A - Student/Pupil Acceptable Use Agreement</td>
<td>32</td>
</tr>
<tr>
<td>Appendix B - Parent/Carer Acceptable Use Agreement</td>
<td>35</td>
</tr>
<tr>
<td>Appendix C - Staff (and Volunteer) Acceptable Use Policy Agreement Template</td>
<td>39</td>
</tr>
<tr>
<td>Appendix D - Record of reviewing devices/internet sites (responding to incidents of misuse)</td>
<td>41</td>
</tr>
<tr>
<td>Appendix E - Reporting Log</td>
<td>42</td>
</tr>
<tr>
<td>Appendix F - Training Needs Audit Log</td>
<td>43</td>
</tr>
<tr>
<td>Appendix G – Students Use of Mobile Devices in lessons Acceptable Use Agreement</td>
<td>44</td>
</tr>
</tbody>
</table>

| Glossary of Terms                                                       | 45   |
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>Activity</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>This online safety policy was approved by the Governing Body/Governors</td>
<td>November 2022</td>
</tr>
<tr>
<td>The implementation of this online safety policy will be monitored by the:</td>
<td>Online Safety Coordinator, Group, Senior Leadership Team</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</td>
<td>Twice a year</td>
</tr>
<tr>
<td>implementation of the online safety policy generated by the monitoring</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td>July 2023</td>
</tr>
<tr>
<td>the light of any significant new developments in the use of the</td>
<td></td>
</tr>
<tr>
<td>technologies, new threats to online safety or incidents that have taken</td>
<td></td>
</tr>
<tr>
<td>place. The next anticipated review date will be:</td>
<td></td>
</tr>
<tr>
<td>Should serious online safety incidents take place, the following external</td>
<td></td>
</tr>
<tr>
<td>persons/agencies should be informed:</td>
<td>LA Safeguarding Officer, Academy Group Officials, LADO, Police</td>
</tr>
</tbody>
</table>

The school will monitor the impact of the policy using:
- Logs of reported incidents - CPOMS
- Monitoring logs of internet activity (including sites visited)/filtering - Smoothwall
- Internal monitoring data for network activity - Smoothwall
- Surveys/questionnaires of
  - students/pupils
  - parents/carers
  - staff

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. 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.

Aims

Our school aims to:
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

**Legislation and guidance**

This policy is based on the Department for Education’s (DfE’s) statutory safeguarding guidance, *Keeping Children Safe in Education*, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE’s guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the National Curriculum computing programmes of study.

At The Appleton School we are aware of the legislative framework under which this online safety policy 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.

Where applicable the school will seek legal advice 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.

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/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
Childnet – Cyberbullying guidance and practical PSHE toolkit:
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children’s Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum
SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection
360data - free questionnaire and data protection self review tool
ICO Guides for Education (wide range of sector specific guides)
DIE advice on Cloud software services and the Data Protection Act
IRMS - Records Management Toolkit for Schools
Roles and Responsibilities

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

Governors/Board of Directors

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
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 Authority relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- 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**

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school’s ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.
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 (including volunteers) and Support Staff (Appendix C):
All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school’s ICT systems and the internet (appendix 3), and ensuring that pupils follow the school’s terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of ‘it could happen here’

This list is not intended to be exhaustive.

All staff, including contractors and agency staff, and volunteers 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/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead/Designated Person/Officer

Details of the school’s designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
Liaising with other agencies and/or external services if necessary
Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

The DSL and deputies 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 (Appendix A):**
- 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 (Appendix B):**
Parents are expected to:
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

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
Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

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.

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:
- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In Key Stage 3, pupils will be taught to:
- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
How to report a range of concerns

By the end of secondary school, pupils will know:
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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

The school will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents’ evenings.

The school will let parents know:
- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

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.
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

- 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 secure)
- 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.
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's guidance for use of mobile phones by students in school can be found in Appendix G
- The school allows:

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

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.

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 is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
• Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/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>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Use of personal email addresses in school/academy, or on school/academy network</td>
<td>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Use of school/academy email for personal emails</td>
<td>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Use of messaging apps</td>
<td>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Use of social media</td>
<td>Not allowed</td>
<td>Not allowed</td>
</tr>
<tr>
<td>Use of blogs</td>
<td>Not allowed</td>
<td>Not allowed</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.

**Cyber-bullying**

**Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

**Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and form tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

**Examining electronic devices**

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils’ electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a ‘good reason’ to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**
If a staff member believes a device may contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE’s latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils will be carried out in line with:

- The DfE’s latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils’ electronic devices will be dealt with through the school complaints procedure.

**Acceptable use of the internet in school**

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices A to C.

**Pupils using mobile devices in school**

At the Appleton School pupils are allowed to bring mobile phone devices to school. This is because many students who travel to school by themselves or use public transport. We also have a number of Young Carers who may be needed to be contactable during the day. Any devices that are brought into school remain the responsibility of the child/parent/carer.

Pupils are not permitted to have their mobile devices out when in the school building.

Pupils are permitted to use their mobile devices during break and lunchtimes whilst outside of the building. There still remains a ‘NO RECORDING’ (video or audio) policy to use of the phones whilst being used.

At the direction of the teacher for classroom activities/trips and visits/educational activities only, pupils are also permitted to use their devices under the following guidelines:

- The student must be seen to use the school WiFi - AppletonWN and then enter username/password
- The phone screen must be visible to the teacher at all times by placing the device flat on the table at all times
- Only the sites/activities directed by the classroom teacher may be used
- Pupils are not to use them to communicate (social media, text, phone call) within the lesson
- Pupils are prohibited to use the camera function on their devices
- The classroom teacher must be able to see what the device is being used for at all times.

Pupils must adhere to the school’s Use of Mobile Devices Policy and the acceptable use agreement for mobile phone use.

**Sanctions**

If a pupil is in breach of any of the above points, they will be subject to the relevant sanctions in line with the whole school Behaviour Policy.

For example:

- If deemed necessary by the classroom teacher the device will be confiscated. (Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act 2006)
If they are confiscated the classroom teacher will confiscate and will then hand the phone to the appropriate member of staff – i.e. pastoral, safeguarding.

The sanctions for mobile phone use link with the school’s wider behaviour policy.

If required staff do have the power to search pupils’ phones, as set out in the DfE’s guidance on searching, screening and confiscation. The DfE guidance allows us to search a pupil’s phone if we have reason to believe the phone contains pornographic images, or if it is being/has been used to commit an offence or cause personal injury. This will only be completed by the designated senior member of staff at the school.

If any inappropriate content is found on a phone, or if there is any inappropriate behaviour it may lead to school having to report to the appropriate agencies.

Pupils and parents are also reminded that certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies as appropriate.

Such conduct includes, but is not limited to:

- Sexting (consensual and non-consensual sharing nude or semi-nude images or videos)
- Upskirting
- Threats of violence or assault
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone’s ethnicity, religious beliefs or sexual orientation

**Staff using work devices outside school**

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always install the latest updates

Staff members must not use the device in any way which would violate the school’s terms of acceptable use, as set out in Appendix C.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

**How the school will respond to issues of misuse**

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in our policies on behaviour, ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school’s ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**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>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 UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges</td>
<td></td>
<td></td>
<td>X</td>
<td></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>X</td>
<td></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>X</td>
<td></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>X</td>
<td></td>
</tr>
<tr>
<td>Pornography</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Promotion of any kind of discrimination</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>threatening behaviour, including promotion of physical violence or mental harm</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Promotion of extremism or terrorism</td>
<td></td>
<td></td>
<td>X</td>
<td></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>X</td>
<td></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)
- 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>Action</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).
Responding to incidents of misuse – flow chart

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.
Other Incidents
It is hoped that all members of the school 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
  - criminally racist material
  - promotion of terrorism or extremism
  - offences under the Computer Misuse Act (see User Actions chart above)
  - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

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

<table>
<thead>
<tr>
<th>Students/Pupils Incidents</th>
<th>Actions/Sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refer to class teacher/tutor</td>
<td>Refer to Head of Department/Year/other</td>
</tr>
<tr>
<td>Refer to Headteacher/Principal</td>
<td>Refer to Police</td>
</tr>
<tr>
<td>Refer to Technical Support staff</td>
<td>Inform parents/carers</td>
</tr>
<tr>
<td>Removal of network/internet access rights</td>
<td>Warning</td>
</tr>
<tr>
<td>Further sanction e.g. detention/exclusion</td>
<td></td>
</tr>
</tbody>
</table>

- **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).**
  - X
  - X
  - X

- Unauthorised use of non-educational sites during lessons

- Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device

- Unauthorised/inappropriate use of social media/messaging apps/personal email

- Unauthorised downloading or uploading of files

- Allowing others to access school/academy network by sharing username and passwords

- Attempting to access or accessing the school network, using another student’s/pupil’s account

- Attempting to access or accessing the school network, using the account of a member of staff

- Corrupting or destroying the data of other users

- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
Continued infringements of the above, following previous warnings or sanctions

Actions which could bring the school into disrepute or 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><strong>Actions/Sanctions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Refer to line manager</td>
</tr>
<tr>
<td>Refer to Headteacher</td>
</tr>
<tr>
<td>Refer to Local Authority/HR</td>
</tr>
<tr>
<td>Refer to Police</td>
</tr>
<tr>
<td>Refer to Technical Support Staff for action re filtering etc.</td>
</tr>
<tr>
<td>Warning</td>
</tr>
<tr>
<td>Suspension</td>
</tr>
<tr>
<td>Disciplinary action</td>
</tr>
</tbody>
</table>

### Staff Incidents

**Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).**

<table>
<thead>
<tr>
<th></th>
<th>Refer to line manager</th>
<th>Refer to Headteacher</th>
<th>Refer to Local Authority/HR</th>
<th>Refer to Police</th>
<th>Refer to Technical Support Staff for action re filtering etc.</th>
<th>Warning</th>
<th>Suspension</th>
<th>Disciplinary action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inappropriate personal use of the internet/social media/personal email</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised downloading or uploading of files</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Careless use of personal data e.g. holding or transferring data in an insecure manner</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliberate actions to breach data protection or network security rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature

Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils

Actions which could compromise the staff member’s professional standing

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school/academy

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

Breaching copyright or licensing regulations

Continued infringements of the above, following previous warnings or sanctions

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don’t want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
• develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

**Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

**Links with other policies**

This online safety policy is linked to our:
- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
Appendix A - Student/Pupil Acceptable Use Agreement

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, 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 (Responsible Network Use Policy)

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:  
Signed:  
Date:  
Parent/Carer countersignature:  
RESponsible Network Use Policy

Rules for Students

You have at your disposal, a network that provides an interactive learning environment. You have easy and direct access to an extremely large collection of information and a range of resources for educational purposes.

You must use this resource with respect. This Responsible Internet and Network Use statement will help to protect students, staff and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and internet use must be appropriate to the student's education.
- Copyright and intellectual property rights must be respected.
- Users are responsible for e-mail they send and for contacts made.
- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
- Anonymous messages and chain letters must not be sent.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private purposes.
- The security systems must not be compromised.
- Students must ask permission to print and should not print directly from the internet. Edit your findings first.
- Never use the Network or Internet without the permission of the member of staff present.
- Irresponsible use may result in the loss of Network and Internet access.
- The anti-cyber bullying code of conduct must be followed.

Having read the 'Responsible Network Use Policy', I accept the conditions stated within and agree that I will support and encourage my child to follow the rules detailed.

Name of Student: ____________________________________________________________

Form: ______________________

Name of Parent/Guardian: ____________________________________________________

Signature: ________________________________________________________________

Date: ______________________
Appendix B - 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 on-line 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’s/daughter’s activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the 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>
</tr>
</thead>
<tbody>
<tr>
<td>Data team</td>
</tr>
<tr>
<td>Electronically under student profile/documents</td>
</tr>
<tr>
<td>7 years after date of leaving</td>
</tr>
<tr>
<td>Shredded/deleted</td>
</tr>
</tbody>
</table>

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

35
Date: .........................................................

**Use of Digital/Video Images**

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

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's 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>How this form will be destroyed.</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: .........................................................

<table>
<thead>
<tr>
<th>As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children.</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>I agree to these images being used:</td>
<td>Yes/No</td>
</tr>
<tr>
<td>• to support learning activities.</td>
<td></td>
</tr>
</tbody>
</table>

36
• 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>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 a request for deletion of the data can be made.</td>
</tr>
</tbody>
</table>

Do you consent to your child to 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.

Yes/No

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.

Yes/No

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.
Appendix C - 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 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:  ..............................................................
Appendix D - 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

...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
**Appendix E - Reporting Log**

Group: .................................................................

<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>What?</td>
<td>By Whom?</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>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

42
### Appendix F - 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>
<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>
Appendix G – Students Use of Mobile Devices in lessons Acceptable use agreement

You must obey the following rules if you bring your mobile phone to school:

1. You may not use your mobile phone during lessons, unless the teacher specifically allows you to.
2. Phones must be switched off (not just put on ‘silent’).
3. You may not use your mobile phone in the toilets or changing rooms. This is to protect the privacy and welfare of other pupils.
4. You cannot take photos or recordings (either video or audio) of school staff or other pupils without their consent.
5. Avoid sharing your contact details with people you don’t know, and don’t share other people’s contact details without their consent.
6. Don’t share your phone’s passwords or access codes with anyone else.
7. Don’t use your mobile phone to bully, intimidate or harass anyone. This includes bullying, harassing or intimidating pupils or staff via:
   a. Email
   b. Text/messaging app
   c. Social media
8. Don’t use your phone to send or receive anything that may be criminal. For instance, by ‘sexting’.
9. Rules on bullying, harassment, and intimidation apply to how you use your mobile phone even when you aren’t in school.
10. Don’t use vulgar, obscene or derogatory language while on the phone or when using social media. This language is not permitted under the school’s behaviour policy.
11. Don’t use your phone to view or share pornography or other harmful content.
12. You must comply with a request by a member of staff to switch off, or turn over, a phone. Refusal to comply is a breach of the school’s behaviour policy and will be dealt with accordingly.
13. Mobile phones are not permitted in any internal or external exam or test environment. If you have a mobile phone, you will be asked to store these appropriately, or turn them over to an exam invigilator, before entering the test room. Bringing a phone into the test room can result in your exam being declared invalid.
14. The teacher always has the authority to allow or prohibit the use of mobile phones in their lessons for learning purposes only.
## Glossary of Terms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUP/AUA</td>
<td>Acceptable Use Policy/Agreement – see templates earlier in this document</td>
</tr>
<tr>
<td>CEOP</td>
<td>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.</td>
</tr>
<tr>
<td>CPD</td>
<td>Continuous Professional Development</td>
</tr>
<tr>
<td>FOSI</td>
<td>Family Online Safety Institute</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioners Office</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>INSET</td>
<td>In Service Education and Training</td>
</tr>
<tr>
<td>IP address</td>
<td>The label that identifies each computer to other computers using the IP (internet protocol)</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>ISPA</td>
<td>Internet Service Providers’ Association</td>
</tr>
<tr>
<td>IWF</td>
<td>Internet Watch Foundation</td>
</tr>
<tr>
<td>LA</td>
<td>Local Authority</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information System</td>
</tr>
<tr>
<td>NEN</td>
<td>National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.</td>
</tr>
<tr>
<td>Ofcom</td>
<td>Office of Communications (Independent communications sector regulator)</td>
</tr>
<tr>
<td>SWGfL</td>
<td>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</td>
</tr>
<tr>
<td>TUK</td>
<td>Think U Know – educational online safety programmes for schools, young people and parents.</td>
</tr>
<tr>
<td>UKSIC</td>
<td>UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.</td>
</tr>
<tr>
<td>UKCIS</td>
<td>UK Council for Internet Safety</td>
</tr>
<tr>
<td>VLE</td>
<td>Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application P</td>
</tr>
</tbody>
</table>