Online Safety Policy

Policy Reviewed:	September 2020
Next Review:	September 2021

Development / Monitoring / Review of this Policy

This Online policy has been developed by a working group made up of:

- *Executive Headteacher*
- *Head Of Schools/Deputy Head/Assistant Heads*
- *Safeguarding Lead*
- *Computing Subject leaders*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Parents and Carers*

Schedule for Development / Monitoring / Review

This Online policy was approved by the *Board of Directors on:*	*October 2016*
The implementation of this Online policy will be monitored by the:	*Senior Leadership Team and Computing Leaders*
Monitoring will take place at regular intervals:	*at least once a year*
The *Board of Directors* will receive a report on the implementation of the Online policy generated by the monitoring group (which will include anonymous details of Online incidents) at regular intervals:	*at least once a year*
The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online or incidents that have taken place. The next anticipated review date will be:	*September 2021*
Should serious Online incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police* **See Appendix1**

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of teachers*
- *students / pupils*
- parents / carers
- *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the *academy* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see **Appendix2**). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *academy* 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 behaviour that take place out of school.

Roles and Responsibilities

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

Governors / Board of Directors:

Governors / Directors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online incidents and monitoring reports. A member of the *Board* has taken on the role of *Child Protection.* The role of the Child Protection Governor will include:

- *regular meetings with the Online Co-ordinator*
- *regular monitoring of online incident logs*
- *regular monitoring of filtering*
- *reporting to relevant Governors / Board*

Head teacher / Principal and Senior Leaders:

The Executive *Headteacher* has a duty of care for ensuring the safety (including Online) of members of the school community, though the day to day responsibility for Online will be delegated to the *Computing Leaders.*

- The Executive Head teacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff. (**See Appendix1**).
- *The Senior Leaders are responsible for ensuring that the Computing Leaders and other relevant staff receive suitable training to enable them to carry out their Online roles and to train other colleagues, as relevant.*

- *The 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 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 Computing Leaders.*

Computing / Online Safety subject leader:

- leads the online committee
- takes day to day responsibility for Online issues and has a leading role in establishing and Reviewing the school online policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online 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 incidents and creates a log of incidents to inform future Online developments,
- meets regularly with Child Protection Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

School Network – provided and support by Bolton Schools ICT (SICT)

Bolton Schools ICT (SICT) are responsible for ensuring:

- that the school's / academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school / academy meets required online technical requirements and any Local Authority / other relevant body Online Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (**See Appendix3**)
- that they keep up to date with online technical information in order to effectively carry out their Online role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher / Senior Leader; Computing subject leader for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current *school / academy*

Online policy and practices

- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the *Headteacher / Senior Leader Online Coordinator* 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 issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online 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*

Child Protection / Designated Safeguarding Lead

should be trained in Online 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
- cyber-bullying

Students / pupils:

- are responsible for using the *academy* digital technology systems in accordance with the Student / Pupil Acceptable User Policy
- 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 cyber-bullying.
- should understand the importance of adopting good online practice when using digital technologies out of school and realise that the *academy's* Online Policy covers their actions out of school, if related to their membership of the school

  Parents / Carers

  Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *academy* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.* Parents and carers will be encouraged to support the *academy* in promoting good online 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 and on-line student / pupil records

Policy Statements

Education – students / pupils

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

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The Online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key Online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- *Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Policy (AUPs) and encouraged to adopt safe and responsible use both within and outside school*

(See Appendices 5, 6, 7 and 8)

- *Staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education – parents / carers

Many parents and carers have only a limited understanding of the online risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line 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*
- *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
(See Appendix12)

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: (select / delete as appropriate)

- A planned programme of formal and informal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online training needs of all staff will be carried out regularly. *It is expected that some staff will identify Online as a training need within the performance management process.*
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.

(See Appendix4)

- *Safeguarding and Computing 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 / INSET days.*
- *Safeguarding and Computing lead (or other nominated person) will provide advice /guidance / training to individuals as required.*

Training – Governors / Directors

Governors / Directors should take part in online training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / Online / health and safety / child protection. 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
For school supported by Bolton Schools ICT:

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 responsibilities:

- Academy 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 academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices.

- **All adults will be provided with a username and password** by *Bolton Schools ICT who will keep an up to date record of users and their usernames.*
- **All users will be provided with a username and password** by *Bolton Schools ICT who will keep an up to date record of users and their usernames.* (If schools subscribe to a SICT school blog all pupils are issue a network / Office365 account as standard.)
- KS1 pupils will be taught the importance of password security

- The "master / administrator" passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Executive *Headteacher* or other nominated senior leader and kept in a secure place (e.g. school safe)
- Schools ICT 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.
- *The school has provided enhanced / differentiated user-level filtering*
- *Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations 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.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A School Personal Data template is available in the appendices to this document. (Schools / Academies should review and amend this appendix, if they wish to adopt it. Schools / Academies should also ensure that they take account of relevant policies and guidance provided by local authorities or other relevant bodies).
The school / academy must ensure that:
It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". **(See Appendix11)**
It has a Data Protection Policy **(See Appendix11)**
It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs) Risk assessments are carried out
It has clear and understood arrangements for the security, storage and transfer of personal data
Data subjects have rights of access and there are clear procedures for this to be obtained
There are clear and understood policies and routines for the deletion and disposal of data
There is a policy for reporting, logging, managing and recovering from information risk incidents
There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

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

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

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

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

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

- Users must immediately report, to the nominated person – in accordance with the school /academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, chat.) must be professional in tone and content. *These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Students / pupils should be taught about Online 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 academy website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. **Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'**. While, Ofsted's Online framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school / academy* 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 limiting access to personal information:
Training to include: 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 *academy* or local authority
Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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 school or outside school when using school equipment or systems.

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	

Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)	X				
On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce				X	
File sharing	X				
Use of social media			X		
Use of messaging apps				X	
Use of video broadcasting e.g. YouTube		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).
(See Appendices 1 and 13)

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police. **(See Appendices 1 and 13)**

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

Have more than one senior member of staff / volunteer 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 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 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 other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

Appendix Acknowledgements

Bolton Safeguarding in Education Team and the Online Safety Group would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Policy Template:

- Representatives from Bolton Schools ICT
- Representatives from Bolton Primary and Secondary Schools
- Representatives from Bolton Healthy Schools
- Representatives from Bolton Community Police
- Southwest Grid for Learning – for the initial development of the policy

- **Appendices**

- Appendix1: Responding to incidents of misuse – flowchart
- Appendix2: School Policy Template – Electronic Devices, Search and Deletion
- Appendix3: School Technical Security Policy
- Appendix4: Staff and Volunteers Acceptable Use Agreement Policy
- Appendix5: Pupil Acceptable Use Agreement template - EYFS
- Appendix6: Pupil Acceptable Use Agreement template – Year1 & Year2
- Appendix7: Pupil Acceptable Use Agreement template – Year3 & Year4
- Appendix8: Pupil Acceptable Use Agreement template – Year5 & Year6
- Appendix9: Community Users Acceptable Users
- Appendix10: Third Party ICT Access and Acceptable User Policy
- Appendix11: School Personal Data Policy
- Appendix12: Links to other organisations and documents
- Appendix13: Online Incident Report
- Appendix14: Use of Digital Images & Video
- Appendix15 Google Cloud System Permission
- Appendix16 Online safety policy checklist
- Appendix17: School Online Committee Terms of Reference
- Appendix18 Glossary of terms
- Appendix19 Legislation