CRAMLINGTON LEARNING VILLAGE

Name of Policy:	**Online Safety Policy**
Overview:	**To protect the safety of students at Cramlington Learning Village online**
Policy presented to:	**Finance & Resources Committee**
Date:	**Summer Term 2018**
Policy ratified by:	**Full Governing Body**
Date:	**Summer term 2018**
Author:	**Philip Spoors, AHT, ICT**

Cramlington Learning Village
Online Safety Policy

Contents:

References: These policies are adapted from the South West Grid for Learning Template Policies and influenced by template policies produced by Northumberland LEA

Review details

This Online Safety policy was approved by the Governing Body / Governors Sub Committee on:	2 February 2018
Revision History	Issue 3 May 2018 Issue 2 February 2018 Issue 1 November 2017
The implementation of this Online Safety policy will be monitored by the:	Online Safety Coordinator and Online Safety Group
Monitoring will take place at regular intervals:	Annually (formally) and informally throughout the year based on surveys, evaluations and discussion
The Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once per term
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	November 2018
Should serious online safeguarding incidents take place, the following external persons / agencies should be informed:	Jill Travers (safeguarding lead) who will then liaise with the appropriate authorities e.g. LEA Safeguarding Officer, Academy Group Officials, LADO, Police

Development and monitoring of this Policy

This Online Safety policy has been developed by the school online safety group made up of:

- Online Safety Coordinator - Mr Phil Spoors
- Headteacher - Mrs Wendy Heslop
- Deputy Head Teacher - Mr Jon Bird
- Teaching staff – Craig Baxter
- Governors – Mr Ian Hall and Mrs Dawn Richardson
- Network Manager – Mr Matt Wilkinson
- Data Manager – Mr Richard Majer
- Parents and Carers – Mrs Dawn Richardson
- Support/Pastoral Staff – Mrs Debra Betham and Mr Matt Wilkinson
- Safeguarding Lead – Mrs Jill Travers
- Students – Digital Leaders Group

Consultation with the whole academy community has taken place through a range of formal and informal meetings including ratification by the school governing body.

The school will monitor the impact of the policy using:

- Logs of reported incidents via behaviour tracker
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students
    - parents / carers
    - staff
- External audits
    - 360 Safe Tool
    - Northumberland County Council Annual Esafety Audit
- Discussion
    - Online safety group meetings
    - Digital Leader/ICT Cabinet meetings

Scope of the Policy

This policy applies to all members of the academy community (including staff, students, 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 Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 cyberbullying or other Online Safety 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 appendix for policy). 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 Safety behaviours 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:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Online Safety Governor and will lead this review. The role of the Online Safety Governor will include:

- regular communication with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings where appropriate
- regular monitoring of online safety incident logs via termly online safety report
- regular monitoring of filtering / change control logs via online safety report
- reporting to relevant Governors meetings

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- 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 flowchart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant academy disciplinary procedures.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator 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 / 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. This will include providing sufficient protected time in which to carry out this role as well as access to web designer time to produce secure online systems to record and monitor online safety incidents.
- The Senior Leadership Team will receive termly monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator:

The designated Online Safety Coordinator:

- 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 and governors
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates/reviews logs of incidents to inform future online safety developments
- communicates regularly with Online Safety Governor and Senior Leaders to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of Governors relating to online safety
- reports regularly to Senior Leadership Team via a termly report and CAM meetings

Network Manager:

The Network Manager is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- school filters are applied and updated on a regular basis and that their 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 network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Coordinator and/or the relevant Learning Manager for investigation / action / sanction
- that systems for monitoring software are implemented and updated as agreed in academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices
- they have read, understood and digitally signed the most recent Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem via the correct channels for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

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 strangers
- potential or actual incidents of grooming
- cyber-bullying

It is important to remember that these are safeguarding issues, not technical issues; the technology simply provides additional means for safeguarding issues to develop.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also contribute towards regular reporting to the Governing Body as appropriate.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- maps and reviews the online safety curricular provision – ensuring relevance, breadth and progression

- the monitoring of network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool and local authority audits

Students:

- are responsible for using the academy digital technology systems in accordance with the Student Acceptable Use Policy
- should 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 safety practice when using digital technologies out of school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website, Virtual Learning Platform and information about national / local online safety campaigns as appropriate. Parents and carers will be encouraged to support the academy 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 online student records
- their children's personal devices inside the academy
- their children's use of 1:1 technology both inside the academy and at home

Community Users

Community Users who access academy systems / website / Learning Platform as part of the wider *academy* provision will be expected to sign a Community User AUA before being provided with access to academy systems.

Policy Statements

Education – Students

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

Online safety will be a focus in all areas of the curriculum and staff will reinforce online safety messages across the curriculum where appropriate. The online safety curriculum will 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 ICT / Computing / Wellbeing / 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 should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by the provision of a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside the academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT team 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 and approved by a member of the senior leadership team.

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

- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings
- High profile events / campaigns e.g. Safer Internet Day
- Directing parents to useful websites

Education – The Wider Community

The academy will provide opportunities for local community groups / members of the community to gain from the academy'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 academy website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, feeder schools

Education & Training – Staff / Support Staff

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.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- It is possible that some staff will identify online safety as a training need within the performance management process and in such situations the academy will provide appropriate additional training.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days as appropriate.
- The Online Safety Coordinator 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 subcommittee / 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 (e.g. SWGfL).
- Participation in academy training / information sessions for staff or parents
- Specific training sessions for governors

Technical – infrastructure / equipment, filtering and monitoring

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

A more detailed Technical Security Template Policy can be found in the appendix.

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of 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 academy technical systems and devices.
- All users will be provided with a username and secure password by the 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 and will be required to change their password approximately each school term
- The “master / administrator” passwords for the academy ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. academy safe)
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly

updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. Note that there are additional duties for schools / academies under the Counter Terrorism and Securities Act 2015 which require schools / academies to ensure that children are safe from terrorist and extremist material on the internet. See appendix for information on "appropriate filtering".
- The academy has provided differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff, students, etc.)
- 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. This system involves contacting the network manager and/or E-Learning coordinator directly so that the incident can be logged, investigated and addressed as appropriate.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested termly. The school infrastructure and individual workstations are protected by up to date anti-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. Hosts of visitors can request a guest wifi password from the IT support team. This password enforces student level filtering (our strictest level) and is changed weekly. All trainee teachers and supply teachers are provided with school accounts and have the same policies in place as teaching staff. They also receive the same training.
- Users (staff / students / community users) and their family members are allowed to use school devices at home for personal browsing, however, must abide by the Acceptable Use Policy while doing so.
- Staff are not allowed to download and install executable files on school devices with exceptions being made for subjects where this is essential to curriculum needs (e.g. Computer Science to view student-created programs).
- No member of staff is allowed to use removable media (e.g. memory sticks / CDs / DVDs) to transfer any personal data unless the media is safely encrypted. Likewise, personal data may not be transferred online (e.g. via email or cloud computing) without being secured (see School Personal Data Policy in the appendix for further detail).

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet which are classified as personal information under GDPR. Such images may provide avenues for cyberbullying 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 via our digital images agreement before photographs or videos of students 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 academy events for their own personal use (as such use is not covered by the General Data Protection Regulation). 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, retention and publication of those images. Those images should only be taken on academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) which states that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The 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.
- It shall be responsible for, and be able to demonstrate, compliance with the principles of GDPR.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- It is registered as a Data Controller with the Information Commissioner’s Office (ICO) for the purposes of the GDPR.
- Responsible persons are appointed / identified - Data Protection Officer (DPO)
- 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 transfer / 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 safekeeping 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 (encrypted memory sticks are available from the online safety coordinator)

- 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

The Personal Data Handling Policy Template in the appendix provides more detailed guidance.

Communications

The table below sets out what is and isn't allowed across the academy in terms of communication technologies.

	Staff & other adults				Students			
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 the academy	Y	Y	Y		Y			
Use of mobile phones in lessons			Y					Y
Use of mobile phones in social time	Y							Y
Taking photos on mobile phones / cameras				Y				Y
Use of other mobile devices e.g. tablets, gaming devices	Y							Y
Use of school Chromebook	Y				Y			
Use of personal email addresses in academy , or on academy network		Y						Y
Use of academy email for personal emails				Y				Y
Use of messaging apps for professional purposes		Y						Y
Use of social media for professional		Y						Y

purposes								
Use of blogs for professional purposes	Y				Y			

Staff and other adults

Communication Technologies	**Details**
Mobile phones	Mobile phones can be brought into school by staff and kept on their person during the day. Personal mobile phones should not be used to contact parents or students. Official school phones should be used for this purpose.
Use of mobile phones in lessons or other relevant student areas	Mobile phones and smart watches should not be used in a lesson other than in the case of an emergency (for example a teacher urgently needs to get hold of a senior member of staff for safety reasons). There should be **no** social use of phones in lessons whatsoever. This extends to other areas when students may be present, for example, social areas and eating areas.
Use of mobile phones in social time	Mobile phones should not be used for personal use during social/break times whilst a member of staff is on duty or visible to students (e.g. in a classroom with students).
Taking photos on mobile phones / cameras	No personal device should be used at all to take photos of students or personal information about students.
Use of other mobile devices e.g. tablets, gaming devices	Staff may bring in personal devices (e.g. a personal laptop or tablet) for use in school providing our technicians set them up securely on our school network so they are subject to the same filters and monitoring as other school devices. Such devices must be used in school for professional purposes only and users must take care not to store any sensitive data on their own personal device.
Use of personal email addresses in academy, or on academy network	Staff should have no need to access their personal email accounts in school during work hours. During social times/breaks staff are encouraged not to use personal email accounts in school unless there is a urgent need to do so. Personal accounts should not be accessed during lessons, on duty or in the presence of any students.
Use of academy email for personal emails	School email services (outlook and Gmail) should not be used to send any personal email. These services are provided for professional use only.
Use of messaging apps	Messaging apps should not be used for personal use during social/break times whilst a member of staff is on duty or visible to students (e.g. in a classroom with students).
Use of social media	Use of personal social media in school is not allowed on any device at any time. If a member of staff is using a social media account for professional purposes (e.g.

	department twitter account) this use must be in line with our staff acceptable use policy.
Use of blogs	Staff are allowed to create and use their own blogs for professional purposes so long as these are in line with our staff acceptable use policy. Use of personal blogs is not allowed during working hours.

When using communication technologies the academy 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 should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g. by remote access).*
- Users must immediately report, to the nominated person – in accordance with the 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 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) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- 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 academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

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

Academy staff should ensure that:

- No reference should be made in social media to students, parents / carers or academy 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 academy social media accounts are established there should be:

- Approval granted 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 academy 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 academy or impacts on the school/ academy, it must

be made clear that the member of staff is not communicating on behalf of the 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
- Under no circumstances should staff communicate with parents, students or their siblings using personal social media.

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 in a professional manner

The academy's use of social media for professional purposes will be checked regularly by the online safety coordinator and/or Online Safety Group to ensure compliance with the school 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 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 /academy context, either because of the age of the users or the nature of those activities.

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

User Actions	**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
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, or any communication regarded as offensive, harassment or of a bullying nature.				X	
Promotion of extremism or terrorism				X	

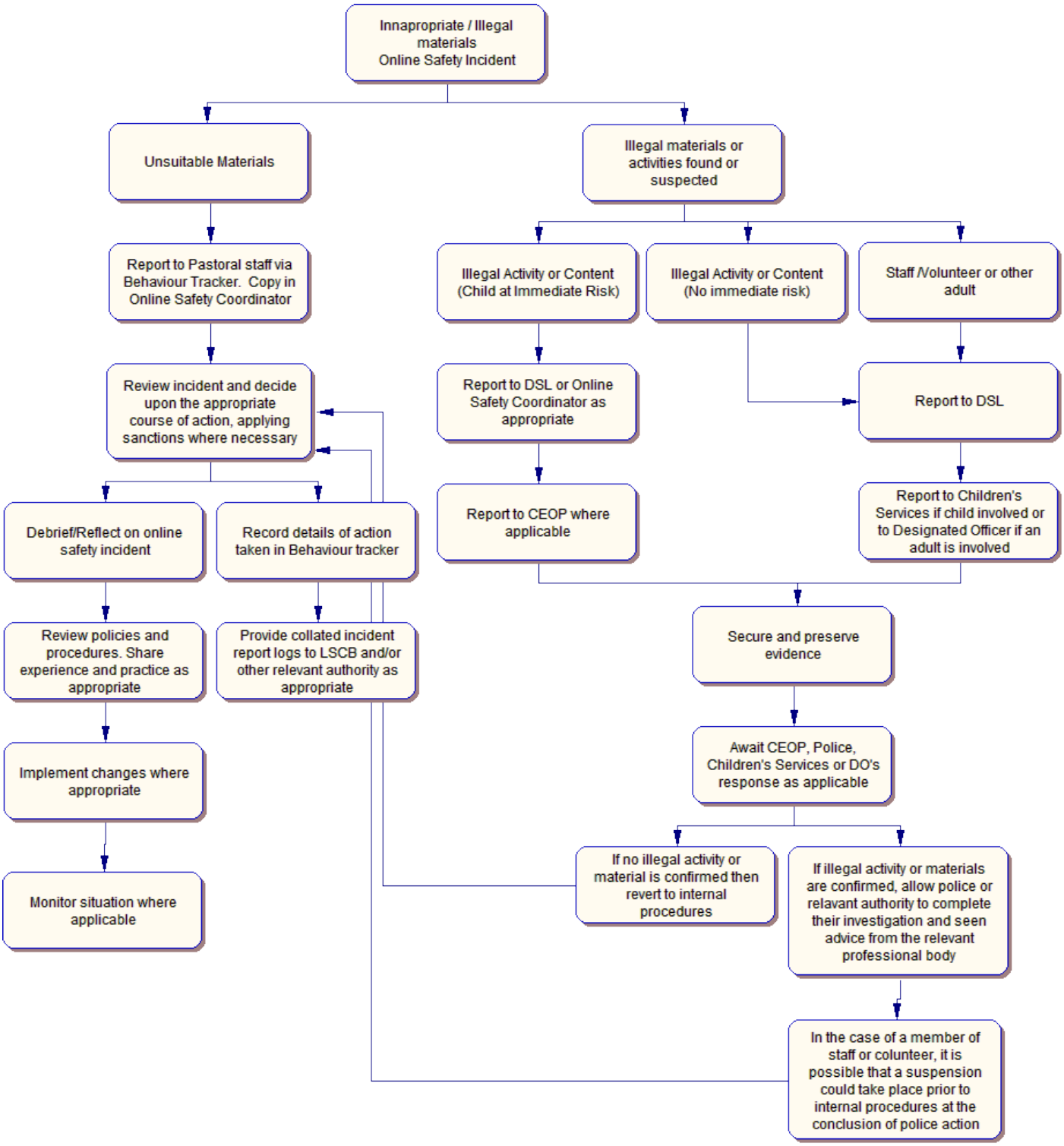
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the 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*			

* For professional purposes only

Responding to incidents of misuse

Illegal Incidents

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



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow 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 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 / Academy 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
    - 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 *academy* 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.

Academy Actions & Sanctions

It is more likely that the academy 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:

Students Incidents	**Refer to pastoral team and online safety coordinator via behaviour tracker**	**Refer directly to safeguarding lead**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X
Unauthorised use of non-educational sites during lessons	X	

Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	
Unauthorised downloading or uploading of files	X	
Allowing others to access academy network by sharing username and passwords	X	
Attempting to access or accessing the academy network, using another student's / pupil's account	X	
Attempting to access or accessing the academy network, using the account of a member of staff	X	
Corrupting or destroying the data of other users	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	
Continued infringements of the above, following previous warnings or sanctions	X	
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the school	X	
Using proxy sites or other means to subvert the academy's filtering system	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X
Taking indecent photographs of self or others	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X
Any online behaviour which puts the student or others at risk of harm	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the General Data Protection Regulation	X	

The pastoral team and/or online safety lead will put the appropriate sanctions in place based on the severity of incidents and taking into account previous incidents. Such actions may include loss of access to the school network / internet, detentions, internal exclusion, contact with parents and in the event of illegal activities involvement of the police.

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Online Safety Coordinator	Refer to Safeguarding lead
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		Only where the incident is of a safeguarding nature
Inappropriate personal use of the internet / social media / personal email	X			
Unauthorised downloading or uploading of files	X		X	
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	X		X	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X		X	
Deliberate actions to breach data protection or network security rules	X		X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X			
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	X		X	
Actions which could compromise the staff member's professional standing	X	X		
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X		

Using proxy sites or other means to subvert the school's / academy's filtering system	X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X
Breaching copyright or licensing regulations	X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X	

Line managers will determine the appropriate sanction based on the severity of incidents and taking into account previous incidents. This may be done in negotiation with the online safety coordinator. Where appropriate they may choose to escalate this to the Headteacher or another member of the senior leadership team. They in turn may refer an incident to the local authority or police if deemed appropriate or necessary.

Appendices

Appendix A
Student Acceptable Use Policies

Student Acceptable Use Agreement - Years 7 to 11

Acceptable Use Policy Agreement

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

For my own personal safety:

- I understand that the school will monitor my use of school ICT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose/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 offline 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 online.

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try 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 systems or devices for online 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 only access online games at appropriate social times and will not access any online games which include inappropriate material, inappropriate language or violence.

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 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 to my own.
- I will not take or share any images or videos 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 not use my own personal devices (mobile phones / USB devices etc.) in school unless I have permission. These devices are usually not allowed unless you have a specific need to use a personal device which has been agreed. I understand that, if I do use my own devices in the school without permission it can be confiscated. On the rare occasion when I do have permission 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/faults involving equipment or software, however this has happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person 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 with the exception of Chrome Store apps on my Chromebook if I opt into the school Chromebook scheme which are not blocked by the school.
- I will not access any social media sites while in school.

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 will 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 cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, internal exclusion, 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

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement above. 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)
- I use my own equipment out of the academy in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student: _____

Group / Class: _____

Signed: _____

Date: _____

Parent/guardian name: _____

Parent/guardian signature: _____

Date: _____

Note that you may be asked to sign this form electronically rather than on paper.

Student Acceptable Use Agreement – Post 16

Acceptable Use Policy Agreement [Agreement to be made electronically]

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

For my own personal safety:

- I understand that the school will monitor my use of school ICT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating online.
- I will consider my digital footprint and aim to have a positive online presence
- 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 offline 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 online.

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try 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 systems or devices for online 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 only access online games at appropriate social times and will not access any online games which include inappropriate material, inappropriate language or violence.

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 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 to my own.
- I will not take or share any images or videos 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:

- When I use my personal mobile devices (laptops / tablets / mobile phones / Chromebooks / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date antivirus software and are free from viruses.
- 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 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 with the exception of Chrome Store apps on my Chromebook if I opt into the school Chromebook scheme which are not blocked by the school.
- I will not access any social media sites while in school.

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 will 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 cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, internal exclusion, 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 [Agreement to be made electronically]

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement above. 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)
- I use my own equipment out of the academy in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student: _____

Group / Class: _____

Signed: _____

Date: _____

Parent/guardian name: _____

Parent/guardian signature: _____

Date: _____

Note that you may be asked to sign this form electronically rather than on paper.

Appendix B
Use of Digital / Video Images

Use of Digital / Video Images

The use of digital images and/or video 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.

The school will comply with the GDPR and request parents / carers 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 own children at school events for their own personal use (as such use in not covered by the GDPR). 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. If you provide consent and later change your mind you are able to do so by contacting the school and we can amend our records.

Digital / Video Images Permission Form [Consent to be given electronically]

Please tick the relevant boxes in all instances to give your consent for photographic images or video of your child being used and sign below

Photographs/video footage of students may be taken and used within lessons or activities to reflect upon learning (seen only by those involved in the activity).	I give my consent for photographs of the named student on this form to be used in this way	☐
Photographs/video footage of students may be taken and used on the school website or in school publications (e.g. school magazine).	I give my consent for photographs of the named student on this form to be used in this way	☐
Photographs/video footage of students may be taken and used in media coverage of the school.	I give my consent for photographs of the named student on this form to be used in this way	☐
Photographs/video footage of students may be taken on field trips/visits/excursions/extracurricular activities and used to showcase these activities.	I give my consent for photographs of the named student on this form to be used in this way	☐

I understand 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. Yes / No

Full name of Student: _____

Parent / Carer's Name: _____

Signature (Parent/Carer): _____ Date: _____

Appendix C
Use of Cloud Systems

Use of Cloud Systems

The school uses Google Apps for Education for pupils and staff. This permission form describes the tools and pupil / student responsibilities for using these services.

The following services are available to each *pupil* and hosted by Google as part of the school's online presence in Google Apps for Education:

Mail - an individual email account for school use managed by the school

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, *we* collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils / students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience and they are essential tools for everyday learning at the school. Please note that these Apps are central to Chromebook use.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Cloud System Permission Form

Parent / Carer's Name: _____

Student Name: _____

As the parent / carer of the above student, I agree to my child using the school using Google Apps for Education. Yes / No

Signed: _____

Date: _____

Appendix D
Staff and Visitors Acceptable Use Policy, Acceptable Use Agreement for Community Users

Staff (and Volunteer) Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, 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 academy 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 student learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement [Agreement to be made electronically]

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 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 academy will monitor all 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, Chromebooks, email, VLE, school Google Apps, 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.
- 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 academy ICT 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 (please refer to our separate policy on Social Networking).
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities or the reputation of the academy.

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

- When I use my personal mobile devices (laptops / tablets / mobile phones / Chromebooks / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date antivirus software and are free from viruses.
- 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 not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 school machine, or store programmes on a school computer, nor will I try to alter school computer settings without permission from the network manager.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy Data Security Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or student 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 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 academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in school, but also applies to my use of 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 academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors 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: _____

Note that you may be asked to sign this form electronically rather than on paper.

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

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

Acceptable Use Agreement

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

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

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines. I understand that if I breach this agreement I may be prohibited from using the school facilities and that any unlawful activities could lead to the school contacting the police or relevant authorities.

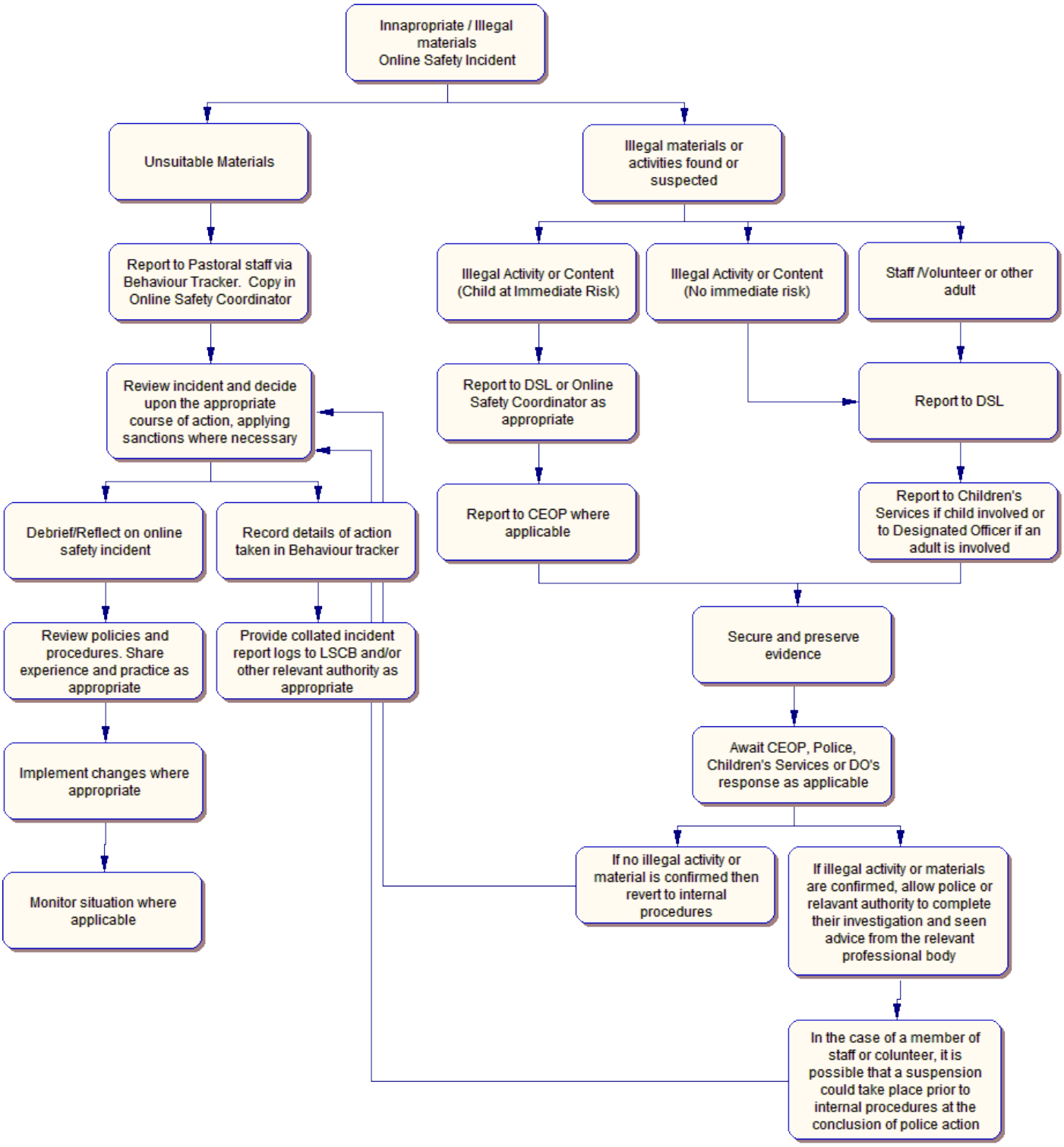
Name: _____

Signed: _____

Date: _____

Appendix E
Responding to Incidents of Misuse, Reporting and Monitoring Logs

Responding to incidents of misuse – flow chart



Reporting and monitoring logs

Inappropriate websites

Inappropriate websites will be monitored by the network manager. This will involve actively looking at reports from our school firewall and filtering systems. It will also involve acting upon feedback from users about inappropriate websites they report.

The network manager keeps a log of websites which have been blocked or unblocked using the built in logging system in our filtering software and firewall.

All breaches and attempted breaches of our school filtering system are automatically logged and reported by Smoothwall. Select users get instant alerts for the most severe safeguarding categories (self-harm, suicide, terrorism, etc.) and pastoral staff also receive weekly reports for their year group. These are acted on as appropriate and any action taken is logged in the appropriate system (behaviour tracker or CPOMS).

Security incidents

The network manager will keep a record of any security incidents which take place on the school systems. This log includes:

- Date and time of the incident
- Description of the incident
- Who was involved in the incident
- Action taken and by whom
- Who reported the incident

Appendix F
Technical Security Policy, Filtering

School Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy
- Logs are maintained of access by users and of their actions while users of the system
- There is effective guidance and training for users
- There are regular reviews and audits of the safety and security of school computer systems
- There is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the school network manager.

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements (the network manager uses local authority meetings and bulletins, government bulletins and advice, Smoothwall advice and a local network of network managers to seek recommendations and best practice)
- There will be regular reviews and audits of the safety and security of school academy technical systems and incidents will be recorded and logged clearly.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to academy technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed at least annually
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their login details and must immediately report any suspicion or evidence that there has been a breach of security.
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Mobile device security and management procedures are in place (for academy provided devices and where mobile devices are allowed access to school systems). Years 7 to 11 only use school chromebooks which are managed through the Google Management console and have no access to the school network. They are subject to all Smoothwall filters on these devices just as they would be on school PCs. At post 16 students can bring in their own mobile device for use in school. These are also filtered through Smoothwall and students connect to the wifi using their school credentials which allows monitoring and recording of their Internet usage. Staff may use personal devices in school but are subject to the same policies outlined for 6th form students above. No access to the school network is possible from any mobile device.
- 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.
- Users will report any actual / potential technical incident directly to the Network Manager (or via the E-Learning coordinator who will pass these details on).
- 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. Hosts of visitors can request a guest wifi password from the IT support team. This password enforces student level filtering (our strictest level) and is changed weekly. All trainee teachers and supply teachers are provided with school accounts and have the same policies in place as teaching staff. They also receive the same training.

- The downloading of executable files and the installation of programmes on school devices will only be undertaken by the school Network manager or technical staff they have delegated this role to.
- Users (staff / students / community users) and their family members are allowed to use school devices at home for personal browsing, however, must abide by the Acceptable Use Policy while doing so.
- Staff are not allowed to download and install executable files on school devices with exceptions being made for subjects where this is essential to curriculum needs (e.g. Computer Science to view student-created programs).
- No member of staff is allowed to use removable media (e.g. memory sticks / CDs / DVDs) to transfer any personal data unless the media is safely encrypted. Likewise, personal data may not be transferred online (e.g. via email or cloud computing) without being secured (see School Personal Data Policy in the appendix for further detail).
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, Trojans, Ransomware, etc.

Password Security

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually.
- All academy networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the academy systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentications for such accounts.
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their login details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users will be allocated by the network manager or their team. Passwords can be changed by all any member of the school IT team or teaching staff.
- Passwords for new users will be issued through an automated process. Enforced changes to passwords are required on a regular basis (every 100 days)
- Users will change their passwords at regular intervals – as described in the staff and student sections below (the level of security required differs for staff and student accounts due to the sensitive nature of data which can be accessed via staff accounts).

Staff Passwords

- All staff users will be provided with a username and password by the school Network Manager who will maintain an up to date record of users and their usernames.
- The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters must not include proper names or any other personal information about the user that might be known by others
- The account should be "locked out" following five successive incorrect logon attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account login
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- The network manager will enforce a password change every 100 days.
- Previous passwords will not be reused for 6 months and the past five passwords cannot be re-used.

Student Passwords

- All users will be provided with a username and password by the school Network Manager who will maintain an up to date record of users and their usernames.
- Students will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in assemblies led by the Online Safety Coordinator
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The Network Manager will ensure that full records are kept of:

- Password changes
- User log-ins
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the school Network Manager who will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to the school E-Learning Coordinator

All users have a responsibility to report immediately to the Network Manager or E-Learning Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The academy use a managed filtering service provided by Northumberland County Council and then further manages its own filtering service to provide enhanced and differentiated filtering for different categories of users. Northumberland use Lightspeed to manage their filtering controls and the school supplements/enhances this with our own Smoothwall filtering.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the nominated Online Safety Coordinator. This process would involve a discussion between the network manager, Online Safety coordinator and the member of staff who has requested the change/temporary change.
- Mobile devices that access the academy internet connection (whether academy or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and discussed with and agreed by the Online Safety Coordinator. If the request is agreed this action will be recorded in a log kept by the Network Manager.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- The Acceptable Use Agreement
- Induction training
- Staff meetings, briefings and insets.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions and newsletters.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering (whether this is carried out in school or by an external filtering provider)
- the grounds on which they may be allowed or denied (schools may choose to allow access to some sites eg social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records / audit of logs)
- any audit / reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the school Network Manager who will decide whether to make school level changes in consultation with senior leaders where appropriate.

Monitoring

The school will produce monitoring logs of incidents where we believe students may have tried to access inappropriate websites. These will be reviewed by both the Network Manager and the Online Safety Coordinator. They will also be passed on to our school pastoral team so that they can follow up where appropriate with individual students.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to the following groups as part of the termly online safety report:

- The Online Safety Group
- Online Safety Governor / Governors committee
- The Senior Leadership team

Where requested this information will also be made available to the Local Authority or Police.

Appendix G
School Personal Data Handling Policy, Electronic Devices – Searching and Deletion

School Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

GDPR lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. GDPR requires organisations to comply with key data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The GDPR defines “Personal Data” as data which relate to a living individual who can be identified (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/)

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines “Sensitive Personal Data” as personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

Policy Statements

The school 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. For more detailed information around this please refer to our separate data retention policy.

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” and retention of records policy.

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

The school's Data Protection Officer (DPO) is Ken Brechin who will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The IAOs (Richard Majer, Data Manager, Phil Spoors, ELearning Coordinator, Matt Wilkinson, Network Manager) will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the GDPR, the school will inform parents / carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers a privacy notice letter. Parents / carers of young people who are new to the school will be provided with the privacy notice through mail.

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process.

Secure Storage of and access to data

The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords and staff passwords will be changed regularly (this is enforced every 100 days). User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left unattended (even for very short periods) and set to auto lock if not used for five minutes. In classrooms teachers may choose to leave resources displayed on screen for students while they walk around the classroom, however, need to ensure that they are not logged into any passworded systems whilst not able to supervise their machine. There is a cookie for online school systems which has a timeout so that sensitive systems cannot be used even if the computer is still logged in.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and encrypted storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

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

- the data must be encrypted and password protected,
- the device must be password protected (encrypted memory sticks are available from the Online Safety Coordinator)
- 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.

The academy has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including backups which are geographically separate to each other. This is all in line with our disaster recovery policy which can be requested if required.

The academy has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the General Data Protection Regulation. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the academy is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The academy recognises that under article 15 of the GDPR, https://gdpr-info.eu/art-15-gdpr/ data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests. A written request to see all or a part of the personal data held by the data controller in connection with the data subject will be sent to the Data Protection Officer. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal

data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should need to use their username and password in order to access the school management information system
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by a responsible individual (Richard Majer).

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Privacy and Electronic Communications

Please refer to the school Freedom of Information Policy

Electronic Devices - Searching & Deletion

The Education Act 2012, the basis of this template, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

Introduction

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. The following technologies are banned in for students in school and can be searched for by authorised school staff (senior leaders and pastoral staff):

- Mobile phones
- Personal tablets
- Personal laptops or Chromebooks not which are not part of the school 1:1 scheme (does not apply at post 16)
- Hand held games consoles or any other gaming device
- Digital cameras
- Digital video recorders
- Digital sound recorders
- Personal MP3 players, iPods or similar

USB drives are not banned for students but may also be searched by authorised school staff. Chromebooks which are part of the school 1:1 scheme may also be searched along with any SD card inside them.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher must publicise the school behaviour policy, in writing, to staff, parents / carers and students at least once a year.

It is recommended that Headteachers (and, at the least, other senior leaders) should be familiar with this guidance.

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

- Jon Bird
- Phil Spoors
- Andy Reeman
- Kim Irving
- Debra Betham
- Lisa Marshall
- Damian Clark
- Jill Travers

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training / Awareness

It is essential that all staff should be made aware of and should implement the school's policy.

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher / Principal to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

The school will already have a policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions. The school should therefore consider including one of the following statements in the policy:

Pupils / students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school in the Online Safety Policy (Communications section). The sanctions for breaking these rules can also be found in this policy.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student being searched.

The authorised member of staff carrying out the search must be the same gender as the student being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student/ pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:

The person conducting the search may not require the pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags.

A student's possessions can only be searched in the presence of the student and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Where the data is to be erased from the student device a copy must be taken first as evidence and this should be documented. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Deletion of Data

A record should be kept of the reasons for the deletion of data / files. Although DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safekeeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).

Audit / Monitoring / Reporting / Review

The responsible person will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

Appendix H
Mobile Technologies Policy

Mobile Technologies Policy

Mobile technology devices may be a school owned/provided or privately owned smartphone, smartwatch, 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.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

The school allows:

Years 7-11

- Chromebooks allocated to students as part of our 1:1 scheme
- Personal Chromebooks which have been authorised for use in school and set up with school filters
- Laptops and tablets which have been authorised for use in school and set up with school filters

Post 16 and Staff

- Chromebooks allocated to students as part of our 1:1 scheme
- Personal Chromebooks, laptops and tablets which have been authorised for use in school

Note that no mobile devices will be allowed full network access which is reserved purely for school desktop devices or school laptops (which are kept in school and not allocated to individuals).

The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices:

- All school devices are controlled through the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user
- Mobile device security and management procedures are in place (for academy provided devices and where mobile devices are allowed access to school systems). Years 7 to 11 only use school chromebooks which are managed through the Google Management console and have no access to the school network. They are subject to all Smoothwall filters on these devices just as they would be on school PCs. At post 16 students can bring in their own mobile device for use in school. These are also filtered through Smoothwall and students connect to the wifi using their school credentials which allows monitoring and recording of their Internet usage. Staff may use personal devices in school but are subject to the same policies outlined for 6th form students above. No access to the school network is possible from any mobile device.
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licensed software etc.
- All school devices are subject to routine monitoring
- Proactive monitoring has been implemented to monitor activity

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device into the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;

- Devices may not be used in official tests or exams
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in school
- Devices must be in silent mode on the school site
- School devices are provided to support learning. It is expected that pupils will bring devices to school as required.
- Confiscation and searching - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended to work is not permitted
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices may be made to ensure that users have not removed required apps
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Devices may be used in lessons in accordance with teacher direction
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- Printing from personal devices will not be possible

Insurance and warranty

School Chromebooks provided as part of our 1:1 scheme come with a three year insurance for accidental damage and theft and an extended three year warranty. Batteries are covered by a one year warranty.

Should a user need to make a claim they should contact a member of the IT support team who will check the device to determine whether an insurance or warranty claim is needed and ensure that the claim will meet the conditions of the insurance company. They will then provide clear instructions as to how to make insurance or warranty claim. Full details of the insurance policy is provided when a parent first opts into the scheme and terms differ from year to year depending on the scheme offered.

Social Media

Please refer to the separate school policy ‘Social Networking Policy and Guidance’.

Appendix I
Legislation

Legislation

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

It is recommended that legal advice is sought in the advent of an e 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.

General Data Protection Regulation 2016

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:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

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

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks 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 a 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 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. 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)