Online Safety Policy

2020-2021

Online Safety Policy

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

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

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

Roles and Responsibilities

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

Governors

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

- meetings with the Online Safety Lead
- reviewing online safety incident logs, filtering and monitoring systems, development plans
- reporting to relevant Governors meetings

Headteacher / Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority disciplinary procedures).
- The Headteacher will ensure that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that the Online Safety Lead is given support by the Designated Safeguarding Lead (DSL). This is to provide a clear link to the wider safeguarding work of the school and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive termly monitoring reports from the Online Safety Lead.

Online Safety Lead

- Will set up and lead and Online Safety working group, made up of a range of staff
- takes day to day responsibility for online safety issues, supported by the school SLT
- has a leading role in establishing and reviewing the school online safety policies / documents and planning for improving school practice
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- liaises with SLT following Online Safety incidents to inform their decisions about any consequences
- meets regularly with the DSL to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team and Governors**Network Manager / Technical staff**

The school currently contracts management of the network to an external contractor. As part of our Service Level Agreement, they ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and digital devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Lead or SLT for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Lead or SLT for investigation / action / sanction, including during any online learning activities
- 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 digital devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these digital 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
- will ensure that any portable digital devices used to store data will be securely encrypted – and that any loss of data is immediately reported to the online safety lead.

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 adults / strangers
- potential or actual incidents of grooming
- online-bullying
- other illegal online activity eg sharing of sexual images

Students / Pupils:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement, including during any online learning activities
- 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 digital devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school , if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile digital devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / app and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- online learning platforms and resources
- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and online student / pupil records
- their children's personal digital devices in the school

Community Users

Community Users who access school IT provision will be expected to sign a Community User AUA before being provided with access to school systems. (A Community Users Acceptable Use Agreement Template can be found in the appendices.)

Development / Monitoring / Review of this Policy

This Online Safety policy will be reviewed in consultation with

- Headteacher / Senior Leaders
- Online Safety Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents and Carers
- Community users

Consultation with the whole school community will take place through a range of formal and informal meetings.
The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring of internet activity / filtering
- Surveys / questionnaires of
    - students
    - parents / carers

Staff Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of the school's 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 should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. The work of the school on British Values will reinforce this.
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile digital 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, app
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g, ThinkUKnow and NetAware.

Education – The Wider Community

The school aims to provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Developing Digital Leaders to support partner primary schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

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

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

Training – Governors

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 school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).
- Training delivered as part of a Governors Meeting

Technical – infrastructure / equipment, filtering and monitoring

The school currently contracts management of the network to an external contractor. As part of our Service Level Agreement, and in partnership with LA technical support services, they ensure that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and digital devices.
- All users will be provided with a username and secure password
- Users are responsible for the security of their username and password and will be required to change their password regularly
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher and Finance Officer.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Any security breach, including data loss, is reported immediately to the Online Safety Lead and SLT in school.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile digital devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- All school laptops and other hardware are encrypted before being given out to staff.

Mobile Technologies (including BYOD)

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

All users should understand that the primary purpose of the use mobile / personal digital devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies
- The school BYOD network is secure, filtered and monitored when available to students in school
- The use of mobile digital devices by students is permitted for learning purposes during lessons
- The school behavior policy covers use of mobile digital devices outside of lesson times
- Education about the safe and responsible use of mobile digital devices is included in the school Online Safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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 is obtained before photographs of students are published on the school website / social media / local press

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Students must not take, use, share, publish or distribute images of others without their permission
- Students' / Pupils' full names will not be used online, particularly in association with photographs.

Data Protection

Please see our Data Protection Policy for further information. It has been reviewed in line with the 2018 GDPR legislation.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other digital 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 digital 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 offer virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

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

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to the Online Safety Lead or SLT 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. 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.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. School s/, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their

employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party – online behavior is covered by our staff code of conduct. Reasonable steps to prevent predictable harm must be in place.
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

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

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- If they are concerned an issue has arisen they should immediately report it to their line manager / SLT who will provide the appropriate support

When official school social media accounts are established there is:

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

Monitoring of Public Social Media

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

The school's use of social media for professional purposes will be checked regularly by SLT / Online Safety Lead to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school / context, either because of the age of the users or the nature of those activities.

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

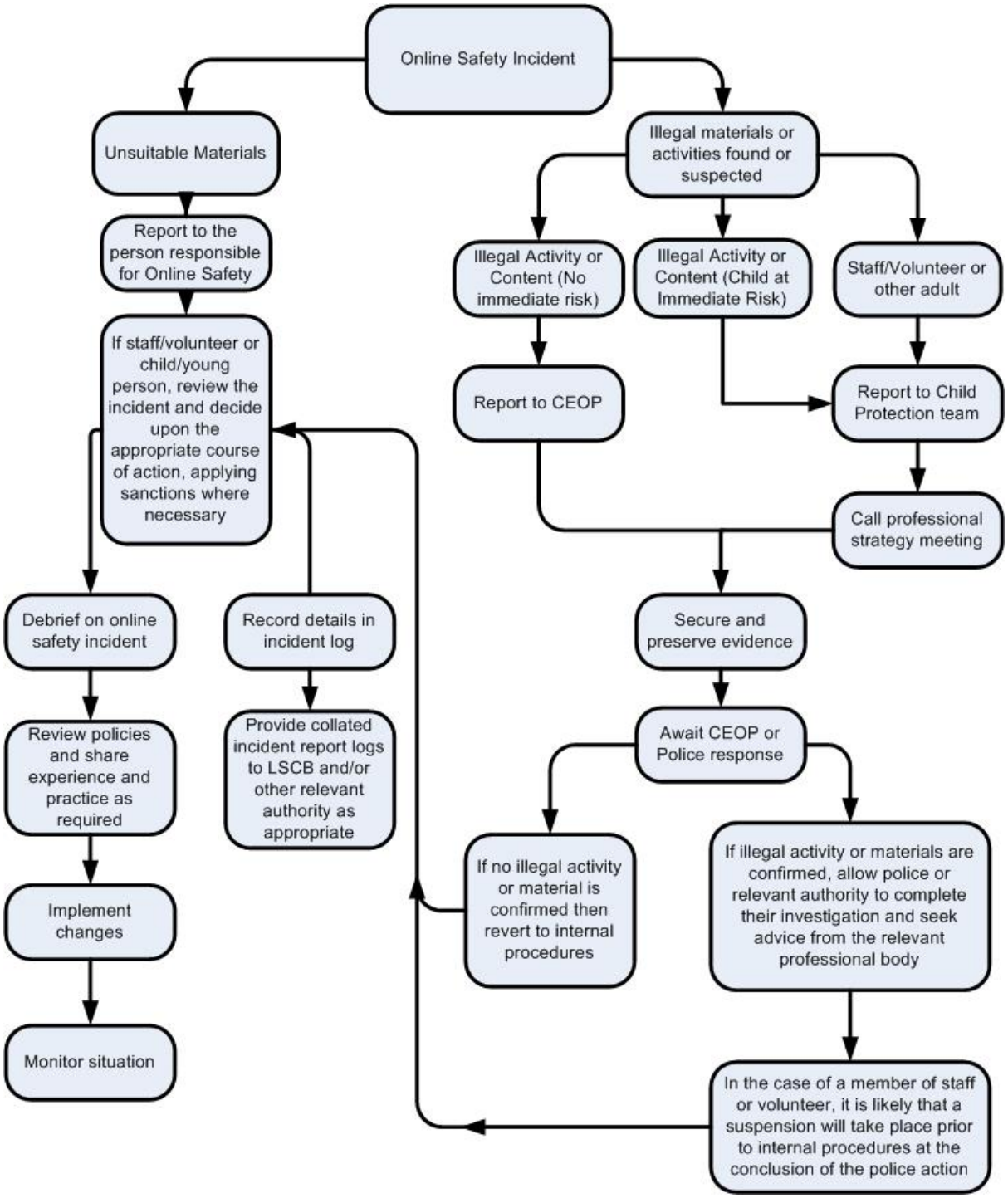
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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 school /					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg 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	

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.
In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If the incident of a safeguarding nature the DSL (or Headteacher) must be informed immediately and they will lead on the incident, supported by other staff as necessary. The Safeguarding policy details our procedures here, including when school must report incidents to the police. In these instances, computers/other digital devices (including phones) should be taken and held securely pending the investigation. If there are suspicions that the incident involves indecent images of children under the age of 18 they should NOT be looked at by staff.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The actions taken should then be recorded securely on CPOMS.

Student / Pupil Acceptable Use Agreement

Denton Community College students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use

For my own personal safety:

- I understand that the school will monitor my use of the systems, digital 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 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, etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line – to parents/carers, school staff or via the CEOP website.

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

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- If I have concerns about another student's use of ICT (eg unsafe or risky behaviour; malicious or inappropriate behaviour online) I will report this to a member of staff to ensure that students at Denton, and our ICT systems, remain safe.

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

- I understand that the school systems and digital devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or digital devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- I understand that any misuse of ICT will be followed up in line with the school behaviour policy

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

- I will only use my own personal digital devices (mobile phones / USB / digital digital devices etc) in school if I have permission.
- I understand that, if I do use my own digital devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment and that my behaviour is still covered by the school behaviour policy.
- 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
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

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

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

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be 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, suspensions, contact with parents and in the event of illegal activities involvement of the police.
- If school has reason to believe any device has been used in illegal or other serious incidents, the device will be confiscated and kept securely while the incident is investigated.

If you do not sign and return this agreement, access will not be granted to school systems and digital devices.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.
I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and digital devices both in and out of school
- I use my own digital devices in the school (when allowed) e.g. mobile phones, tablets, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, social media, etc.

Name of Student / Pupil: .....

Signed: .....

Date: .....

DCC Staff (and Volunteer) Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

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

Introduction:

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 school will monitor my use of school digital technology & communications systems.
- I understand that the rules set out in this agreement also apply to use of technologies (e.g. laptops, email, social media etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school code of conduct.
- 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 only write down/store a password securely.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of.

I will be professional in my communications and actions when using school 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 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 staff code of conduct.
- 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 on-line activity that may compromise my professional responsibilities or the reputation of the school. 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).

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

- When I use my mobile digital devices (laptops / tablets / mobile phones / USB digital devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment – including encryption and passwords. will ensure that any such digital devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted or if I have any concerns about the validity of the email
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, 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/attempt to install programmes or store programmes on a computer.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, or any other issues involving my use of ICT, however this may have happened.

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

- I understand that this agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

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 digital devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: ..... Signed: .....

Date: .....

DCC Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and digital devices
- that school systems, digital 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 digital devices

Acceptable Use Agreement

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

- I understand that my use of school systems and digital 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 school 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 school has the right to remove my access to school systems / digital 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 digital devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ..... Signed: .....

Date: .....

Parent / Carer Acceptable Use Agreement

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

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. (School need to decide whether or not they wish parents to sign the Acceptable Use Agreement on behalf of their child)

Permission Form
Parent / Carers Name: .....
Student / Pupil Name: .....

As the parent / carer of the above students / pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

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

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

Signed: .....

Date: .....

Use of Digital / Video Images

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

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

The school will comply with the Data Protection Act and request parent or 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 children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

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

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

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

Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital / Video Images Permission Form

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

As the parent / carer of the above student / pupil, I agree to the school taking digital / video images of my child / children.	Yes / No
I agree to these images being used:	
• to support learning activities.	Yes / No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
Insert statements here that explicitly detail where images are published by the school /	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....

Date: .....

Use of Cloud Systems Permission Form

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

School s will need to review and amend the section below, depending on which cloud hosted services are used.
The school uses *insert cloud service provider name* for pupils / students and staff. This permission form describes the tools and pupil / student responsibilities for using these services.

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

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

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

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

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

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

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

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

Use of Biometric Systems in England and Wales

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

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

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card. The school has carried out a data privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

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

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

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

Parent / Carers Name: .....

Student / Pupil Name: .....

As the parent / carer of the above student / pupil, I agree to the school using biometric recognition systems, as described above.	Yes / No
I understand that the images cannot be used to create a whole fingerprint / palm print of my child and that these images will not be shared with anyone outside the school .	Yes / No

Signed: .....

Further guidance

- Each parent of the child should be notified by the school that they are planning to process their child's biometrics and notified that they are able to object.
- In order for a school to process children's biometrics at least one parent must consent and no parent has withdrawn consent. This needs to be in writing.
- The child can object or refuse to participate in the processing of their biometric data regardless of parents' consent.

- School s and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.
- Permission only needs to be collected once during the period that the student attends the school but new permission is required if there are changes to the biometric systems in use.

Student / Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student / Pupil Acceptable Use Agreement.

It is suggested that when the Student / Pupil AUP is written that a copy should be attached to the Parents / Carers AUP Agreement to provide information for parents and carers about the rules and behaviours that students have committed to by signing the form.