Online Safety Policy

Review by policy owners:	Ben Croton, Chris Hayward, Tamsin Lowe, Oliver Bates (Online safety policy review group), December 2021 – February 2022
Review by Trustees:	Helena McVeigh (Specialist Trustee) Doug Croucher (Policy Review Trustee) March 2022
Ratified by Board of Trustees:	29 March 2022
Next review date:	January 2023

Within this policy the term CEO refers to the CEO of the Trust. The term Headteacher refers to the Headteacher of the School.

The Trustees of the Twynham Learning Trust (the Trust) are Charity Trustees and Company Directors and for the purpose of this policy these terms are interchangeable.

This policy reflects the legislation at the time that it was last reviewed. Any changes in legislation will take precedence over anything printed in this policy.

Contents

1. Statement of intent

Twynham Learning understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Twynham Learning has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

2. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following Trust-wide (T) and School (S) policies:

- Child Protection and Safeguarding Policy (T)
- Data Protection Policy (T)
- Special Educational Needs and Disabilities (SEND) Policy (T)
- Behaviour Policy (S)
- Anti-Bullying Policy (S)
- Code of Conduct for Staff & Volunteers (T)
- Remote Learning Policy (T)

3. Scope of the Policy

This policy applies to all members of Twynham Learning school communities (including staff, pupils, volunteers, parents, LAB members and Trustees, visitors and community users) who have access to and are users of school ICT systems, both in and out of the school.

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

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

4. Roles and responsibilities

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

4.1 LAB members and Trustees

LAB members and Trustees are responsible for monitoring the Online Safety Policy and for reviewing the effectiveness of the policy. Regular information about online safety incidents and monitoring reports will be provided to governors. An Online Safety Governor will be appointed within each school and their role will include:

- regular contact with the Online Safety Coordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- reporting to the Student Welfare Committee or Local Advisory Board, as appropriate

4.2 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 Coordinator.

- 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 Section 5.2.1 – “Responding to incidents of misuse” and relevant HR / other relevant body 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.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

4.3 Online Safety Coordinator

The Online Safety Coordinator:

- leads the Online Safety Group
- has responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- liaises with the DSL
- 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 school technical staff
- ensures that a log of incidents is maintained to inform future online safety developments
- liaises regularly with the Online Safety LAB member to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

4.4 Network Manager / IT Manager

The Network Manager/IT Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any other relevant body Online Safety Policy/Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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/Gateway/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Coordinator for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

4.5 Teaching and Support Staff (including volunteers)

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement (see appendices)
- they report any suspected misuse or problem to the Designated Safeguarding Lead and/or relevant staff member with responsibility for online safety for investigation/action/sanction
- all digital communications with pupils/parents 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
- pupils understand and follow the Online Safety Policy and acceptable use policies

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where pupils need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked, staff can request that the Technical Staff 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. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

4.6 Designated Safeguarding Lead

The DSL will 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 online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

4.7 Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the LAB.

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

- the production/review/monitoring of the Online Safety Policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree Safe self-review tool

4.8 Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- are responsible for seeking help from school staff if they are concerned about something they or a peer have experienced online
- are responsible for reporting online safety incidents and concerns

- 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 Online Safety Policy covers their actions out of school, if related to their membership of the school

4.9 Parents and Carers

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The schools will take every opportunity to help parents understand these issues through parent information evenings, newsletters and a dedicated Online Safety website portal. Parents will be encouraged to support the Trust 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/Gateway and online pupil records

5. Education and training

5.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the Trust'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 is provided as part of Computing/PD (PSHE) /other lessons and are regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

5.2 Education – Parents and Carers

Parents play an essential role in the education of their children and in the monitoring/ regulation of children's online behaviours. However, keeping up-to-date with the ever-changing online safety risks and issues is a real challenge. 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 Trust will therefore seek to provide information and awareness to parents through:

- Curriculum activities
- Parent information evenings
- Newsletters
- A dedicated Online Safety website portal via the school website

5.3 Education – The Wider Community

The Trust will provide opportunities for local community groups / members of the community to gain from the Trust'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

5.4 Education & Training – Teaching and Support Staff (including 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 Coordinator (or other nominated person) 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
- The Online Safety Coordinator (or other nominated person) will provide advice/guidance/ training to individuals as required

5.5 Training – LAB members

LAB members should take part in online safety training/awareness sessions, which may be offered in a number of ways:

- Attendance at training provided by the 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)

6. Technical infrastructure

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users (at KS2 and above) will be provided with a username and secure password by IT Services who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The ‘administrator’ passwords for the school ICT system, used by the Network Manager/I.T. Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- The Network Manager/ IT 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 licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (e.g. 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 should ensure that children are safe from terrorist and extremist material when accessing the internet
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils etc.)
- Twynham Learning 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
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software
- An agreed procedure is in place for the provision of temporary access of ‘guests’ (e.g. trainee teachers, supply teachers, visitors) onto the school systems
- An agreed procedure is in place regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on school devices that may be used out of school
- An agreed procedure is in place that controls the extent to which staff can download executable files and install programs on school devices
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

7. Use of Emerging Technologies

7.1 Mobile Technologies (including BYOD/BYOT for Staff, Visitors and Sixth Form Pupils)

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

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant Trust or school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-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 Trust Acceptable Use Agreements for staff, pupils and parents will give consideration to the use of mobile technologies
- The Trust allows:

	School Devices (LAC/SEN, Sixth Form, Staff)			**Personal Devices**		
	School owned for single user	**School owned for multiple users**	**Authorised device**[1]	**Student owned (6th form only)**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*			
Internet only				*Yes*	*Yes*	*Yes*
No network access						

7.2 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils 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 Trust 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 pupils 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
- Parents will be given the opportunity to opt out of consenting for photographs of their child to be published on the school website/social media/local press

[1] Authorised device – purchased by the student/family through a school-organised scheme, such as Clingan's Trust. This device may be given full access to the network as if it were owned by the school.

- In accordance with guidance from the Information Commissioner's Office, parents 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 made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Trust and 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
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Trust into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Pupils' work can only be published with the permission of the student and parents

7.3 Data Protection

This is covered separately in the Data Protection Policy, which includes guidance relating to online safety.

7.4 Communication Technologies

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

	Staff & other adults				**Pupils** (Sixth Form only)			
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 school	✓				✓			
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓					✓		
Taking photos on mobile phones / cameras		✓				✓		
Use of other mobile devices e.g. tablets, gaming devices	✓						✓	
Use of personal email addresses in school, or on school network	✓					✓		
Use of school email for personal emails				✓				✓
Use of messaging apps	✓					✓		
Use of social media	✓					✓		
Use of blogs	✓					✓		

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users must immediately report, to the nominated person – in accordance with the Trust 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 pupils or parents (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Pupils will be provided with individual school email addresses for educational use
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

7.5 Social Media - Protecting Professional Identity

All schools and academies have a duty of care to provide a safe learning environment for pupils and staff. Schools and the Trust could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or the Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The Trust 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
- Providing training 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 pupils, parents 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 the Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

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

Personal Use:

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

Monitoring of Public Social Media:

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

The school’s use of social media for professional purposes will be checked regularly by the Online Safety Group to ensure compliance with Trust and school policies.

8. Responding to incidents of misuse

8.1 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 Trust 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 Trust policy restricts usage as follows:

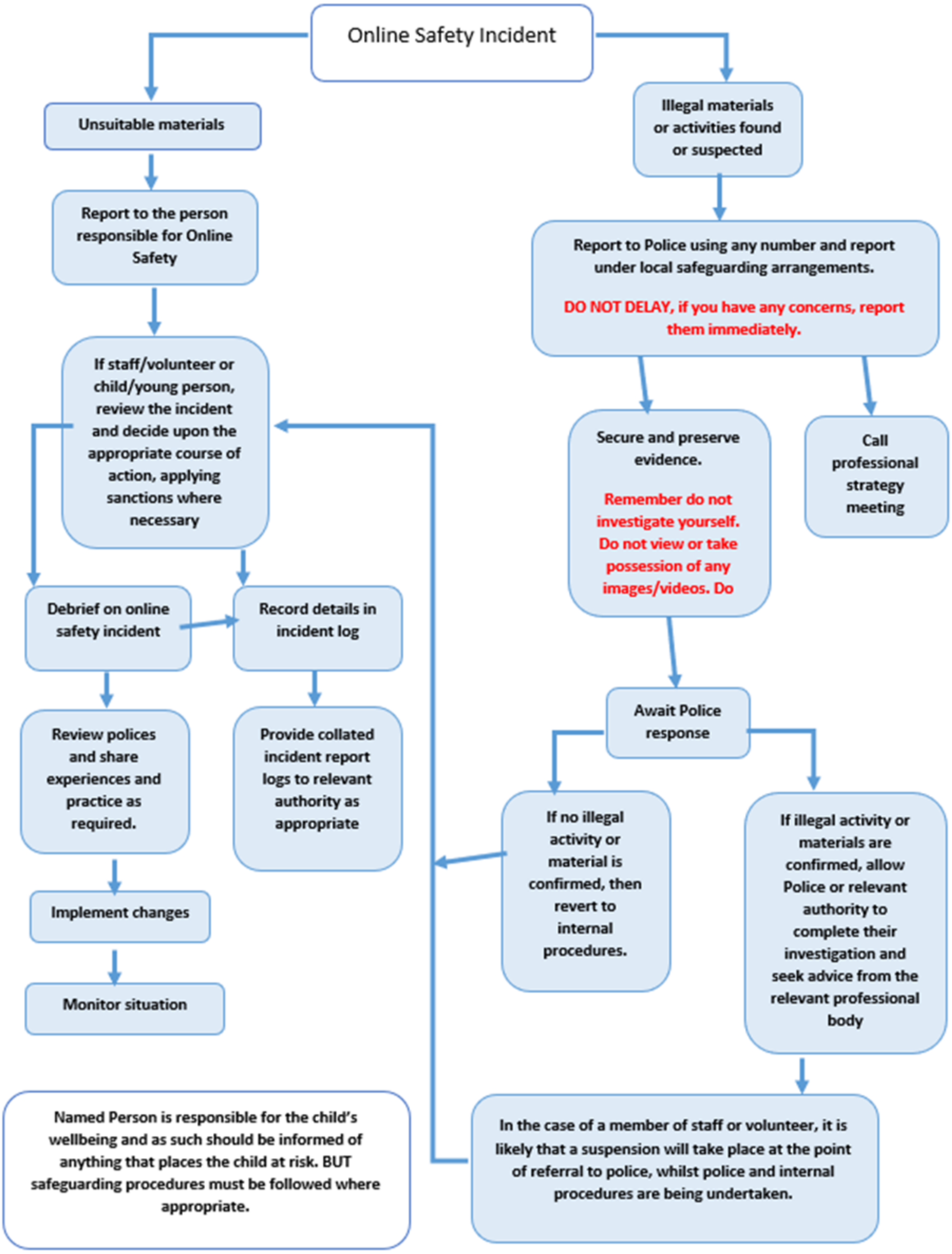
User Actions		Unacceptable and illegal	Unacceptable	Acceptable at certain times	Acceptable for nominnmated users	Acceptable at all times for all users
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978	✓				
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.	✓				
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008	✓				
	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	✓				
	Pornography		✓			
	Promotion of any kind of discrimination		✓			
	Threatening behaviour, including promotion of physical violence or mental harm	✓				
	Promotion of extremism or terrorism	✓				
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Trust or brings the Trust into disrepute		✓			
Using school systems to run a private business			✓			
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school			✓			
Infringing copyright		✓				
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)			✓			
Creating or propagating computer viruses or other harmful files		✓				
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)			✓			
Online gaming (educational)				✓		
Online gaming (non-educational)			✓			
Online gambling			✓			
Online shopping/commerce, file sharing, use of social media, use of messaging apps, use of video broadcasting (e.g. YouTube)				✓		

8.2 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).

8.2.1 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.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

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

8.2.2 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 the Trust / national or 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 school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

8.3 School Actions & Sanctions

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

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

Staff Incidents	Actions					Sanctions
	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓	✓
Inappropriate personal use of the internet / social media / personal email	✓	✓			✓	
Unauthorised downloading or uploading of files	✓				✓	✓
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	✓				✓	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓				✓	
Deliberate actions to breach data protection or network security rules	✓	✓	✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓				✓
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils	✓	✓				
Actions which could compromise the staff member's professional standing	✓	✓	✓			✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓				✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓				✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓

9. Remote learning

All remote learning is delivered in line with the Trust's Pupil Remote Learning Policy.
Schools in consultation with IT technicians will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.
Schools in consultation with IT technicians will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.

- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

Schools will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

10. Peer-on-peer sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Up skirting, i.e. taking a picture underneath a person’s clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment.

Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

11. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer’s attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel ‘special’, particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. Schools will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.
CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.
Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

12. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.
Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. Schools will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.
Positive impacts:

- creates a sense of social support, connectedness and positive interaction, which can boost mental health
- helps to foster and sustain relationships with friends and family, especially those who live far away
- provides a way to make new friends and connections with peers who share similar interests or experiences
- helps some young people to be more open and honest with their friends about how they think and feel
- makes some young people feel supported and less alone during tough times, as they can read about other people's similar experiences
- empowers young people with disabilities or communication needs through creating a sense of community and belonging
- helps children and young people to learn how to strengthen their mental health and keep themselves well
- provides easier access to informal and formal support – help that is available at different times of the day
- Provides a platform on which to be creative and have fun

There are potential risks that social media and the internet can have on children and young people's mental health, which may also affect their ability to thrive and achieve.

Negative impacts:

- Disrupted sleep - Children who use social media at night may not be getting enough sleep. This can not only impact on their learning at school, but a lack of sleep can also increase the risk of depression and anxiety. Children aged 5-16 need to get between 11 hours and 9 hours of sleep a night.
- Accessing harmful or inappropriate content - Children may access content that is violent, racist, hateful or features pornographic material. Studies show that the majority of children and young people are more likely to initially stumble across pornography through targeted adverts or content, rather than intentionally searching for it. When they first accessed pornography, young people were most likely to report that they felt curious, but also shocked, confused or disgusted.
- Cyberbullying - Children and young people may carry out or be exposed to bullying behaviour online. Like bullying offline, cyberbullying also increases a child's risk of developing depression and lowered self-esteem. Research has found that children and young people who experience cyberbullying are twice as likely to self-harm.
- Body image - In a survey conducted by the Mental Health Foundation, 40% of young people (26% of boys and 54% of girls) said that images on social media had made them worry in relation to their body image. Children and young people may compare themselves to celebrities, bloggers or people they are inspired by and begin to filter or manipulate images of themselves to conform to "body ideals" that are often promoted online. Body dysmorphia disorder is when a child or young person persistently worries about aspects of their body or how they look – this can have a huge impact on their life.

Click link for further information: Internet and social media : Mentally Healthy Schools

13. Appendices

Appendix 1 Acceptable Use Agreement – Pupils

Appendix 2 Acceptable Use Agreement – Staff

Appendix 3 Acceptable Use Agreement – Parents

Appendix 1

ICT Acceptable Usage Agreement – Pupils

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

This Acceptable Usage Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Pupil Acceptable Usage Agreement
I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of ''stranger danger'' when I am communicating online.
- I will not disclose or share personal information about myself or others when online (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 online, 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 (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 devices for online gaming, 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 act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's file, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

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 cyberbullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, isolation/exclusion, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Usage Agreement. If you do not sign and return this agreement access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school).
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the school 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, Gateway, website etc.).

Name of Pupil…………………………………………………………………………………………………….TutorGroup…………………………

Signed……Date……………………………………

Appendix 2

Acceptable Use Agreement – Teaching and Support Staff

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.
This Acceptable Use Agreement is intended to ensure:

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

The school will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.
For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Gateway etc.) out of school, and to the transfer of personal data (digital or paper-based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I understand that my ID card facilitates privileged access to buildings and equipment and should be secured at all times and immediately reported if lost
- I will immediately report the loss/theft of my device issued by the school

I will be professional in my communications and actions when using school IT 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 (eg on the school website / Gateway) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents 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.
- I will ensure that any devices issued to me by the school will be stored securely and are stored in a protective case when not in use or being transported

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB 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. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school / academy policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- 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 school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school 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. This could include a warning, a suspension, referral to Governors and / or the trust 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 Name: ____

Signed: ____

Date: ____

Appendix 3

ICT Acceptable Usage Agreement – Parents

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

This Acceptable Usage Agreement 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 are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. The Student Acceptable Usage Agreement is included here, so that parents will be aware of the school expectations of the young people in their care.

Parents are requested to sign the agreement form below to show their support of the school in this important aspect of the school's work.

Parent Acceptable Usage Agreement

Name of Parent ……

Name of Student ………

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

I know that my son/daughter has signed an Acceptable Usage 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 Usage Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed………Date………………………………………