Royds

#LIVE LOVE LEARN

Online Safety Policy

Aspiration: Dream Big
If your dreams don't scare you, they aren't big enough!

Resilience: Be Determined
Resilience is a skill, not an ability. It can be learnt.

Respect: Communicate with Kindness
Manners cost nothing but mean everything.

Initiative: Solve Problems
Every problem is a gift – without problems we would not grow.

Reflective: Never Stop Learning
Never stop learning because life never stops teaching.

1. Introduction

This policy applies to all members of the school community including staff, students, volunteers, parents / carers, visitors, community users, who have access to and are users of school ICT systems, both in and out of the school. It is created with thanks to the SWGfL from their materials for schools.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. 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.

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.

2. Roles and Responsibilities

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

2.1 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 Pupil Support Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor which also encompasses online safety. The role includes:

- regular meetings with senior safeguarding staff to discuss online safety.
- attendance at Online Safety Group meetings.
- regular monitoring of online safety incident logs.
- regular monitoring of filtering / change control logs.
- reporting to relevant Pupil Support Committee meetings.

2.2 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 Co-ordinator i.e. Designated Safeguarding Lead.
- and Business Manager are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- is 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.
- will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. This will be delivered through the school's safeguarding supervision systems.

The Senior Leadership Team will receive safeguarding monitoring reports including data from the Online Safety Co-ordinator.

2.3 Online Safety Coordinator

The Designated Safeguarding Lead (DSL) will assume the role of Online Safety Coordinator as part of the DSL responsibilities. They will however be supported by the school's Safer Schools Police Officer and Technical Services Manager (a CEOP ambassador) who can both provide specialist knowledge and input which can be applied to the wider safeguarding context of any incident.

The Online Safety Coordinator role, in conjunction with the Deputy DSL / Online Safety Coordinator, includes:

- leading the Online Safety Group.
- taking day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- providing training and advice for staff.
- liaising with the Local Authority / relevant body.
- liaising with school technical staff.
- receiving reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meeting regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends the Pupil Support Committee.
- reports regularly to Senior Leadership Team.

2.4 Technical Services Manager and IT Team

The Technical Services 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 Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network, internet, learning platforms, remote access, email or other online system is regularly monitored in order that any misuse / attempted misuse can be reported to the appropriate member of staff.
- that monitoring software and systems are implemented and updated as agreed in school policies

2.5 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 (AUP).
- they report any suspected misuse or problem to the appropriate person.
- all digital communications with students, parents or carers should be on a professional level and only carried out using official school systems within the guidance outlined in the Safer Working Practices Policy.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the Online Safety Policy and acceptable use policies.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

2.6 Designated Safeguarding Team

The Safeguarding Team are 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 or radicalisation.
- cyber-bullying.

2.7 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 the Online Safety Policy, including the impact of initiatives. This will form part of the school's safeguarding supervision infrastructure however with specialist input and school community representation. The group will also be responsible for regular reporting to the Pupil Support committee.

Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the production, review and monitoring of the school Online Safety Policy, documents and systems.
- the production, review and monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- Inputting to the mapping and reviewing the online safety curricular provision; ensuring relevance, breadth and progression.
- monitoring network, internet and incident logs.
- consulting stakeholders including parents / carers and the students about the online safety provision.
- monitoring improvement actions identified through use of the 360 degree safe self-review tool.

2.8 Students

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy.

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online 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.

2.9 Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet or mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website or learning platform and information about national or local online safety campaigns or literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website or learning platform and online student records.
- ensuring their own postings online and on social media role model communicating with kindness.

2.10 Community Users

Community Users who access school systems, website, learning platform etc as part of the wider school provision will be expected to sign a Community User Acceptable User Agreement before being provided with access to school systems.

3. Education: Students

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

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

- A planned online safety curriculum is provided as part of Computing, Digital Literacy and PHSE and other lessons where appropriate.
- Key online safety messages are reinforced as part of a planned programme of assemblies.
- Students are taught in all lessons to be critically aware of the materials or content they access online and are guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Students are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so or bypass is auditable with clear reasons for the need.

4. Education: Parents / Carers

Many parents and carers have 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 and regulation of their children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities.
- Materials such as letters, newsletters, website etc.
- Parents and Carers evenings or sessions.
- High profile events or campaigns e.g. Safer Internet Day
- Reference to the relevant websites or publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers.

5. Education: Wider Community

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

- Online safety messages targeted towards the wider family as well as parents.
- The school website will provide online safety information for the wider community.
- Supporting community groups and local primary schools with their online safety obligations.

6. Education: Staff and 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:

- Staff are given regular updates as and when required.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Coordinator, Safer Schools Police Officer and Technical Services Manager will receive regular updates through attendance at external training, online events and by reviewing guidance documents released by relevant organisations.
- The Online Safety Coordinator, Safer Schools Police Officer and Technical Services Manager will provide advice, guidance or training to individuals as required.

7. Training: Governors

Governors will take part in online safety training or awareness sessions as appropriate with particular importance for those who are members of the Pupil Support Committee. 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 or information sessions for staff or parents. This may include attendance at assemblies / lessons.

8. Technical: Infrastructure, Equipment, Filtering and Monitoring

The school is responsible for ensuring that the school infrastructure (this includes network, cabling, servers, hardware, software and cloud services) is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Further details are available in the Technical Security Policy however key points are summarised below:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements as outlined in Local Authority or other relevant body policy and guidance.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are be securely located and physical access restricted within the physical limitations of the school site.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT Team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password as required).
- The “master / administrator” passwords for the school ICT system, used by the Technical Services Manager (or other person) are available to the Headteacher or Business Manager and kept in a secure place.
- The Technical Services Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced and differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Users to report any actual or potential technical incident or security breaches either through CPOMS or the IT Helpdesk depending on the nature of the incident.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of guests e.g. trainee teachers, supply teachers, visitors, onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- Staff are unable to use removable media 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. Office 365 negates the need for this.

9. Mobile Technologies

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

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The Mobile Technologies Policy is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding and Child Protection 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 is an integral part of the school's Online Safety education programme.

The Mobile Technologies Policy provides further details on the use of personal devices in school however key points are summarised below.

The school allows:

	School Devices			Personal Devices		
	Single User	Multiple User	Authorised Device	Student Owned	Staff Owned	Visitor Owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	No	No	No	No	Yes	On request
No network access	No	No	No	Yes	No	No

10. 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 or 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 will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained at the start of term for the publication of photographs of students on the school website, social media or newsletters however students will also be asked for consent at the time a photo is taken. At this time, a student is also expected to alert staff if permission has been declined for photo publication. Any photo that will be used in a higher profile way e.g. stock PR photos or in the local press will be subject to individual consent.
- In accordance with guidance from the Information Commissioner's Office, parents or carers are welcome to take videos and digital images only of their own children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites.
- Staff and volunteers are allowed to take digital or video images to support educational aims or celebrate success 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 normally be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work which identifies an individual will only normally be published with the permission of the student.

11. Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations. Separate policies are in place to address the requirements and further details can be found within them.

12. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. It is currently felt that the use of mobile phones by students in school is counterproductive in most situations and leads to behaviour and safeguarding risks. This is outlined in the Behaviour Policy. There are however occasional subjects e.g. Photography, where mobile phones can be used with a teacher's permission. Students

should assume that they are not permitted to use phones unless they have received an explicit instruction from their teacher.

It is accepted that the nature of working in a school means that access to personal accounts or personal communications is not possible. To support staff and their work life balance, the school accepts the occasional use of school addresses and technology for personal use however this should be kept to a minimum, be discrete and not be to the detriment or jeopardise school equipment or reputation. No controversial views should expressed using a school email addressed and all communication should show respect and embody the school value of Communicate with Kindness.

The following points should also be noted:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students 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 Technical Services Manager, DSL or Senior Leader, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students are taught about online safety issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information is not to be posted on the school website and only official email addresses used to identify members of staff.

13. Social Media: Protecting Professional Identity

The school has a duty of care to provide a safe learning environment for students and staff. Refer to the school's Social Media Policy and Safer Working Practices guidance for further detail however the school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through:

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

School staff ensure that:

- No reference should be made in personal social media to students, parents or carers or school staff. School accounts will not make such mention without their consent.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions are 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

Official school social media accounts are managed in the following way:

They are set up by the Business Manager and linked to generic school email addresses and passwords that are held by the Technical Services Manager.
There are clear processes for the administration and monitoring of these accounts involving at least two members of staff, including one Senior Leader.
There is a code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse and understanding of how incidents may be dealt with under school disciplinary procedures.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken. The school permits reasonable and appropriate access to private social media sites.

Monitoring of public social media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school.
- The school will effectively respond to social media comments made by others according to a defined policy or process.
- Where possible, the school will act to protect the interests of both school and staff in response to offensive and derogatory posts. It should however be understood that there are limitations to what can be done based on UK law and the laws of the countries where platforms are hosted.

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

14. Unsuitable or 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 normally 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	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 or calls a person's suitability to work with children into question				X	
Using school systems to run a private business					X	
Using other systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Using approved temporary access codes to access incorrectly filtered content.				X		
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)*					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage - downloading / uploading large files that hinders others in their use of the internet*					X	
Online gaming; educational			X			
Online gaming; non-educational					X	
Online gambling					X	
Online shopping			X			
File sharing other than through Office 365*					X	
Use of social media				X		
Use of unapproved messaging apps or video conferencing platforms*					X	
Use of video broadcasting e.g. YouTube			X	X		

*with the exception of IT staff responding to incidents

15. 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.

If there is any suspicion that the website(s) concerned may contain child abuse images or if there is any other suspected illegal activity, the Safer Schools Police Officer will manage the incident.

16. 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 will be followed:

- More than one senior member of staff involved in this process. This will normally involve the Technical Services Manager and on occasions the Safer Schools Police Officer. 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. The same computer will be used for the duration of the procedure where possible.
- 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 and signed except in the case of images of child sexual abuse.

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.
- Police involvement and/or action.

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Safer Schools Police Officer 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.

The computer or files will immediately be isolated.

17. School Actions and Sanctions

It is more likely that the school will 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 or disciplinary procedures.

Incidents involving students could involve:

- Deliberately accessing or trying to access material that could be considered illegal (see above).
- Unauthorised use of non-educational sites during lessons.
- Unauthorised or inappropriate use of mobile phone, digital camera or other mobile device.
- Unauthorised or inappropriate use of social media, messaging apps or 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 or other system 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.
- Deliberate vandalism or damage to IT hardware or peripherals.

This list is not exhaustive. Where appropriate incidents will be dealt with under the published Stages of Behaviour system. Sanctions can include the removal of IT use or bills being raised to parents for damage caused. It should however be noted that certain incidents may be so serious that they have to be reported to the police for further action.

Incidents involving staff could involve:

- Deliberately accessing or trying to access material that could be considered illegal (see above).
- Inappropriate personal use of the internet, social media or 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 or text messaging to carrying out digital communications with students.
- 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.

- Failure to communicate with kindness in online activities.
- 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.
- Exposing students to inappropriate content.
- Deliberately accessing or trying to access offensive or pornographic material.
- Breaching copyright or licensing regulations.
- Deliberately using IT systems in a manner intended to provide false or misleading information or entering / manipulating data to achieve this effect.
- Continued infringements of the above, following previous warnings or sanctions.

This list is not exhaustive. Where appropriate incidents will be dealt with under the school's Disciplinary Policy. It should however be noted that certain incidents may be so serious that they have to be reported to the police or LA Safeguarding Teams for further action.

18. Cyber Bullying

All forms of bullying, including cyber bullying, are taken very seriously. A key school value is respect, communicate with kindness. Bullying is never tolerated and it is not acceptable for any member of staff or a student to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Grievance or Anti-Bullying and could result in disciplinary action.

This doesn't just extend to behaviour within the work place. In some instances, bullying or harassment that occurs outside the school where there is a link to employment or being a student could also fall under the responsibility of the employer or school and therefore result in disciplinary action being taken against the responsible individual.

Certain activities relating to cyber bullying could be considered criminal offences under a range of different laws. Cyber bullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice-based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

If an allegation is received that a member of staff or student is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another member of the school community, the school will investigate this matter. Any allegation of bullying or harassment made against another member of our community where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, may be dealt with through the Anti-Bullying or Grievance Policy and could lead to disciplinary action.

Staff and students are required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts .
- Staff not befriending students and young people on social networking services and sites.
- Keeping personal phone numbers private.
- Staff not using personal phones to contact parents and students and young people
- Keeping personal phones secure, i.e. through use of a pin code.
- Not posting information about themselves that they wouldn't want employers colleagues, students, young people or parents to see
- Not retaliating to any incident

- Keeping evidence of any incident
- Promptly reporting any incident using existing routes for reporting concerns.

Staff in schools, as well as students, may become targets of cyberbullying. No one should ever retaliate to, i.e. personally engage with, cyberbullying incidents. They should report incidents appropriately and seek support.

Staff should report all incidents to the designated line manager or member of their school senior management team and students should report them to their pastoral team or any adult they feel comfortable speaking to. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

Royds