Ham Dingle Primary School
Part of United Learning

ONLINE AND E-SAFETY POLICY

Policy Start Date – September 2021

Policy Review Date – September 2022

Reviewed by – Governors

Date Approved -

Author – Simon Wilkinson (Computing Co-ordinator/Online Safety Lead)

Rationale

The requirement to ensure that staff, children and young people are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools/ academies are bound.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see Electronic Devices – Search and Deletion Policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and responsibilities

Governors/Board of Directors:

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

- regular meetings with the Online Safety Co-ordinator/officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meetings

Head teacher and Senior Leaders:

The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.

The Head teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority/MAT/other relevant body disciplinary procedures).

The Head teacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Head teacher and 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 will include annual CPD and allocated time for monitoring. 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 Lead.

Online safety Lead:

At Ham Dingle, the Online Safety Lead (OSL) is **Mr Simon Wilkinson.** He works closely with the senior leadership of the school and the designated safeguarding lead to monitor and implement this policy. His main responsibilities include:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/MAT/relevant body
- liaises with school technical staff
- Liaises with DSL to receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

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/academy online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement (AUP/AUA) - in Appendix.
- They have read and signed to confirm they have understood the most recent guidance specified in Keeping Children safe in Education 2019
- they report any suspected misuse or problem to the Head teacher/ Senior Leader/Online Safety Lead/ DSL for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online 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
- 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
- Pupils understand that there are sanctions for inappropriate use of technologies and the academy will implement these sanctions in accordance to the behaviour policy
- Pupils understand that academy may investigate any reported misuse of systems by pupils out of school hours as part of safeguarding procedures

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying
- liaise with the online safety lead

Students/Pupils:

Pupils have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure, monitored and safe system. Pupils:

- are responsible for using the academy digital technology systems in accordance with the student/pupil acceptable use agreement which they and their carers will be expected to sign before being given access to school systems
- 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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's online safety policy covers their actions out of school, if related to their membership of the school
- Should understand that the school has a duty of care to all pupils. Misuse of non-school provided systems, out of school hours, will be investigated by the school in line with the behaviour, anti-bullying and safeguarding policies.

Parents/carers

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

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

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school/academy (where this is allowed)

Parents/ carers will be responsible for:

- endorsing (by signature) the pupil acceptable use agreement
- ensuring that cameras on their mobile phones are not used on school premises during school meetings or without consent

Community Users

Community Users who access academy systems or programmes as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to school/academy systems.

- Ham Dingle Academy will ensure that user restrictions are in place to safe guard pupils and staff considering carefully what they are prepared to provide community access to
- Guest access to the internet in the academy will be subject to the same filtering rules as other academy users.
- If the school provides access to school/academy software, they need to ensure that the software is not copied or used inappropriately.
- There will be no access to pupil or staff data/information unless relevant parties have agreed in line with GDPR. The academy has the right to refuse the use of, or may wish to check portable storage devices such as memory sticks, external hard drives, before they are attached to the academy network.

Policy Statements

Education – Students/Pupils

There is a planned and progressive E-Safety Curriculum. We have adopted the Switched On Computing scheme which includes e-safety in every lesson as well as focus lessons every half term for every year group. All staff have a responsibility to promote good online practices.

- A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and should be regularly revisited – this includes the use of ICT and new technologies in and outside the academy.
- Key online safety messages should be 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 on-line and are 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 educated about the dangers and impact of sexting, cyber-bullying and radicalisation during PSHE lessons and assemblies. They will know how to seek help if they are affected by any form of online bullying or exploitation. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies – parent/carer, teacher/trusted member of staff; NSPC, CEOP.
- Pupils are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside academy when using ICT, the internet and mobile devices.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. SafeSearch is set up on RMUnify for children to use.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- SMART rules are displayed in learning environments and children's planners.

Education – Parents/carers

The academy provides information and awareness of online safety to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- Online/E-safety workshops
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

Education - Extended Schools/Wider Community

The academy offers family support in Online Safety/E-Safety so that parents/carers and children can together gain a better understanding of these issues. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff/Volunteers

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

- Annually, 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 receive online safety training as part of their induction programme, ensuring that they fully understand the academy online safety policy and acceptable use agreements.
- The Online Safety Lead and DSL receive regular updates through attendance at external training events (e.g. from SWGfL/LA/United Learning/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 annually in staff meetings/training sessions.
- The Online Safety Lead and DSL will provide advice/guidance/training to individuals as required.

All staff are familiar with the academy policy including:

- Safe use of e-mail
- Safe use of the internet including use of internet-based communication services, such as instant messaging and social network or any other academy approved system
- Safe us of the academy network, including the wireless network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones, iPads and digital cameras
- Publication of pupil information/photographs/videos/posts/bogs/calendars and information available on the academy website
- Capturing and storing photographs/videos/audio files on personal and academy owned devices
- Cyberbullying procedures
- Their role in providing e-safety education for pupils
- The need to keep personal information secure.

All staff are formally update about E-safety matters at least once a year during annual Safeguarding CPD.

Training – Governors/Directors

Governors are invited to take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This is offered through:

- Attendance at training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation.
- Participation in school/academy training/information sessions for staff or parents
- Invitations to attend lessons, assemblies and focus days.

Technical – infrastructure/equipment, filtering and monitoring

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

1. Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements

2. There will be regular reviews and audits of the safety and security of academy technical systems
3. Servers, wireless systems and cabling must be securely located and physical access restricted
4. All users will have clearly defined access rights to academy technical systems and devices.
5. All users (at KS2 and above) will be provided with a username and secure password by Simon Wilkinson (Computing co-ordinator) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. KS1 children and below will be given generic passwords.
6. The administrator passwords for the academy systems, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. academy safe/personal OneDrive)
7. Rachel Garratt (Business Manager) and Simon Wilkinson are 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
8. Internet access is filtered for all users. Smoothwall filtering is in place according to DGfL policy. 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.
9. Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. E-Safe is currently used by RM/DGfL.
10. The academy has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc)
11. Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
12. If any user is concerned about any actual/potential e-safety concerns they are to report it to Simon Wilkinson (OSL) and Cath Feane (DSL). See Safeguarding Policy for procedures.
13. 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 devices are protected by up to date virus software. These are managed by RM/UL.
14. Authorisation by the head teacher is needed for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
15. A guardianship document is signed before academy owned equipment leaves the premises. This clearly outlines the user’s responsibilities.
16. An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices – part of AUP.
17. Authorisation is required by the head teacher for use of portable storage devices such as USB sticks – these are banned apart from guests delivering training to staff.
18. Staff have been trained on using Sharepoint and OneDrive on home computers. They can access the documents saved onto these cloud locations but must not save

any data to their own personal device. Any work done at home must be through the online platforms.

Mobile Technologies (including BYOD)

The academy has provided technical solutions for the safe use of mobile technology for academy devices:

- All academy devices are controlled through the use of Mobile Device Management software - *currently in operation for student devices.*
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The academy has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at an academy location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- All academy devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

Personal devices are not permitted access to the academy wireless.

Academy chain computers have a separate SSID on the wireless network where they can automatically log on to the network. Only specified individuals (Simon Wilkinson, Phil Sugars, Robin Pyman) have access to administrative rights on the Ham Dingle Academy network.

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/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment; the personal equipment of staff must 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 academy 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 students/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.
- Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

Ham Dingle Academy has a Data Protection Policy that meets statutory requirements.

Personal data is recorded, processed, transferred and made available according to the current data protection legislation.

Ham Dingle Academy ensures that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school/academy may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it

- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- it provides staff, parents, volunteers, teenagers and older children with information about how the academy looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- Procedures are in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- The IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with academy policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile devices these must be encrypted and password protected.
- will not transfer any academy personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Communications

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

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

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

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual academy 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 academy website and only official email addresses should be used to identify members of staff.
- Under no circumstances should a member of staff contact a pupil or parent/carer using their personal device unless authorised by the Head teacher.
- The academy is not responsible for the loss, damage or theft of any personal mobile device.
- The academy provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via a Learning Platform.

Social Media – Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school/academy or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

- Risk assessment, including legal risk

Academy staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the academy or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The academy 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 should effectively respond to social media comments made by others according to a defined policy or process

School use of social media:

- Only select members of staff are given admin rights to post to the school's social media websites (Facebook, Twitter and Class Dojo)
- Permission from parents is sought for any photos/videos of children uploaded to the sites

More information can be found on our Social Media Use Policy.

Dealing with unsuitable/inappropriate activities

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

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices						X

• Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) **Any criminal offence will automatically be referred to the police and appropriate authorities.**					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce			X		
File sharing		X			
Use of social media			X		
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube			X		

Sexting

Definition: the production and/or sharing of sexual photos and videos of and by young people whoa re under the age of 18. (UKCCIS, 2016) This does not include the sharing of sexual photos and videos of under-18 year olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

What to do if an incident involving 'sexting' comes to your attention

Report to the DSL (Cath Feane) immediately.

- **Never** view, download or share the imagery yourself, or ask a child to share or download – **this is illegal.**
- If you have already viewed the imagery by accident (e.g. if a young person has shown it to you before you could ask them not to), report this to the DSL.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- **Do not** share information about the incident to other members of staff, the young person(s) it involved or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

- **Follow normal Safeguarding procedures to report to the DSL.**

Responding to incidents of misuse

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Policy, parents/carers will be called into the academy for a meeting with the OSL/DSL
- Further misuse of the agreement will result in not being allowed to access the internet for a period of time and a meeting arranged with parents/carers with the OSL/DSL/Head teacher to discuss the matter
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials, the child should report this to an adult immediately and take appropriate action to minimise the window so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, the can use the CEOP button to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies will be addressed by the OSL/DSL/Head teacher.

Children will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

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) for responding to online safety incidents and report immediately to the police.

Acceptable Use Policy for Staff and Volunteers

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Simon Wilkinson the Online Safety Lead (OSL).

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the OSL, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

By signing the form below I agree that...:

I will only use the school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.

I will only use the approved, secure email system(s) for any school business.

I will ensure that personal data (such as data held on Integris) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

I will not install any hardware or software without seeking permission from the Headteacher.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.

I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

I will respect copyright and intellectual property rights.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….. Date ……

Full Name ……..(printed) Job title . . . . . .