BRIGANTIA
LEARNING TRUST
Creating excellence together

Online Safeguarding Policy

Including Social Media Policy

To be reviewed Autumn 2017

Document Control

Any questions regarding this document should be directed to:
enquiries@hindehouse.net

Name	Position	Date
	Online Safeguarding Team	September 2015
	Online Safeguarding Team	September 2016
	Online Safeguarding Team	November 2016

Contents

Policy Introduction

Online Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The online world is rapidly developing and many of our children have access to devices which enable them to connect to the internet, take images, videos and communicate with others.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the use of these new technologies can put users at risk. The breadth of issues within online safeguarding is considerable, but they can be categorised into three areas of risk:-

Content: being exposed to illegal, inappropriate or harmful material
Contact: being subjected to harmful online interaction with other users
Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Many of these risks reflect situations in the off-line world so it is essential that this Online Safeguarding Policy is used in conjunction with other policies including the Trust safeguarding and child protection policies

The Multi-Academy Trust must demonstrate that it has provided the necessary safeguards to help ensure that in all our schools everything has been done that could reasonably be expected to manage and reduce these risks. The online safeguarding policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people, children, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

Communication of the Policy

- Each school`s senior leadership team are responsible for ensuring all members of staff and pupils are aware of the existence and contents of the school Online Safeguarding policy and the use of any new technology within school.
- The Online Safeguarding policy is provided to and discussed with all members of staff formally.
- All amendments are published and awareness sessions are held for all members of the school community.
- An Online Safeguarding module is included in the PSHE and Computing and IT curriculum in all schools covering and detailing amendments to the Online Safeguarding policy.
- An Online Safeguarding training programme is established across the Trust to include a regular review of aspects of the Online Safeguarding policy.
- Online Safeguarding training is part of the transition programme across the Key Stages and when moving between establishments, pupils' responsibilities regarding the school Online Safeguarding policy is reviewed.
- The key messages contained within the Online Safeguarding policy are be reflected and consistent within all acceptable use agreements in place within the schools.
- We endeavour to embed Online Safeguarding messages across the curriculum whenever the internet or related technologies are used
- The Online Safeguarding policy is introduced to the pupils at the start of each school year
- Safeguarding posters will be prominently displayed around the school
- Links to relevant information and reporting buttons can be found on the website and VLE, including The Sharp System.

Roles and Responsibilities

In the Brigantia Learning Trust, we believe that Online Safeguarding is the responsibility of all the school communities, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team:

- The Executive Principal and Headteachers have overall responsibility for online safeguarding all members of the school community, though the day to day responsibility for online safeguarding will be delegated to the Safeguarding Lead – Anne Robson and deputy coordinators in each school:

    - Concord – Nicola Sherwood
    - Hinde House Primary – Charlene Bennett, Adrian Keeling
    - Hinde House Secondary – Sue Flynn, Karole Cotterell, Diane Greenwood
    - Wincobank – Tracey O'Malley

  Supported by the Trust Technical Team:
    - Dave Riley
    - Adam Kubica

- The headteachers or senior leadership teams are responsible for ensuring that the Online Safeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safeguarding roles and to train other colleagues when necessary.
- The headteachers or senior leadership teams ensure that there is a mechanism in place to allow for monitoring and support of the Online Safety coordinators or deputies.
- The senior leadership teams will receive monitoring reports from the Online Safeguarding Coordinator.
- The headteachers or senior leadership teams should ensure that they are aware of procedures to be followed in the event of a serious Online Safeguarding incident. (see flow chart on dealing with online safety incidents- Appendix A)

Responsibilities of the Online Safeguarding Trust Team

- To ensure that the school Online Safeguarding policy is current and pertinent.
- To ensure that the school Online Safeguarding policy is systematically reviewed at agreed time intervals.
- To ensure that school Acceptable Use Agreements are appropriate for the intended audience.
- To promote to all members of the Trust community the safe use of the internet and any technologies deployed within school.
- To monitor the coverage of e-safeguarding across all schools

Responsibilities of the Online Safeguarding Coordinator, Deputies and Safeguarding Lead

- To promote an awareness and commitment to Online Safeguarding throughout the school.
- To be the first point of contact in school on all Online Safeguarding matters.
- To take day-to-day responsibility for Online Safeguarding within school and to have a leading role in establishing and reviewing the school Online Safeguarding policies and procedures.
- To communicate regularly with IT technical staff.
- To communicate regularly with the designated Safeguarding Directors.
- To communicate regularly with the senior leadership teams.
- To create and maintain Online Safeguarding policies and procedures.
- To develop an understanding of current Online Safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in Online Safeguarding issues.
- To ensure that Online Safeguarding education is embedded across the curriculum.
- To ensure that Online Safeguarding is promoted to parents and carers.
- To liaise with the schools safeguarding staff who will contact local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on Online Safeguarding issues to the senior leadership teams.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safeguarding incident.
- To ensure that an Online Safeguarding incident log is kept up to date.

Responsibilities of the Teaching and Support Staff

- To read, understand and help promote the school's Online Safeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy and sign the Acceptable Use Agreement.
- To report any suspected misuse or problem to the Online Safeguarding coordinator.
- To develop and maintain an awareness of current Online Safeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed Online Safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of Online Safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the school.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by transferring data through secure communication systems.

Responsibilities of Technical Staff

- To read, understand, contribute to and help promote the school's Online Safeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Agreement.
- To report any Online Safeguarding related issues to the Online Safeguarding coordinators.
- To develop and maintain an awareness of current Online Safeguarding issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in the personal use of technology.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school`s ICT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices. The responsibility for "Bring Your Own Device" (BYOD) belongs to the owner of the device.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Protecting the professional identity of all staff, work placement students and volunteers

Communication between adults and between children / young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

Responsibilities of Staff:

When using digital communications, staff should:

- Only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- Not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- Not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child/young person on social networks.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Be careful in their communications with children so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring the school into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Safeguarding Officers

- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

Responsibilities of Pupils

- To read, understand and adhere to the school pupil Acceptable Use Agreement.
- To help and support the school in the creation of Online Safeguarding policies and practices and to adhere to any policies and practices the school creates.
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies on the use of mobile phones.

- To know and understand school policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss Online Safeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the school in promoting Online Safeguarding.
- To read, understand and promote the school pupil Acceptable Use Agreement with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss Online Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology.
- To agree to and sign the admissions form which clearly sets out the use of photographic and video images outside of school.

Responsibilities of the Board of Directors

- To read, understand, contribute to and help promote the school's Online Safeguarding policies and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the Online Safeguarding Trust team in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in Online Safeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its Online Safeguarding strategy.

- To use Trust email systems to enable secure receipt of information.

The role of the Safeguarding Directors includes:

- Regular meetings with the E-Safeguarding Co-ordinators
- Regular monitoring of e-safeguarding incident logs
- Reporting to Governors meeting

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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- We provide a series of specific Online Safeguarding-related lessons in every year group as part of the PSHE and Computing and IT curriculum.
- We celebrate and promote Online Safeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We discuss, remind or raise relevant Online Safeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use is carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils are taught how to use a range of age-appropriate online tools in a safe and effective way.
- Pupils are reminded about their responsibilities through an Acceptable Use Agreement which every pupil sign.
- Staff model safe and responsible behaviour in their own use of technology during lessons.
- Pupils are taught how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils are guided to use age-appropriate search engines. All use is monitored and pupils are reminded of what to do if they come across unsuitable content.
- All pupils are taught in an age-appropriate way about copyright in relation to online resources and are taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils are taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils are made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline, the CEOP report abuse button or the Sharp System.

All Staff (including Directors)

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

- A planned programme of formal e-safeguarding training is made available to staff.
- An audit of the e-safeguarding training needs of all staff is carried out regularly.
- All new staff receive e-safeguarding training as part of their induction programme, ensuring that they fully understand the school e-safeguarding policy and Acceptable Use Agreement.
- This E-Safeguarding policy and its updates are presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safeguarding Coordinator (or other nominated person) in each school provide advice / guidance / training to individuals as required.

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 and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through

- Parents' evenings
- Newsletters
- Letters
- Website/VLE

Managing ICT systems and access

The school is responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

- All access to school ICT systems should be based upon a 'least privilege' approach.
- Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software are kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and is kept active and up to date.
- The school agree which users should and should not have internet access and the appropriate level of access and supervision they should receive. At Key Stage 2, pupils have an individual user account with an appropriate password which is kept secure, in line with the pupil Acceptable Use Agreement. They will ensure they log out after each session.

Passwords

The Trust has a responsibility to ensure that all elements of our schools' infrastructure and network equipment is as safe and secure as possible. All staff and pupil access to school-owned equipment and information assets should be controlled through the use of appropriate username and password complexity policies. It is important that all pupils and staff have an awareness of how to construct a complex and secure password as well as understanding the security implications of not protecting the password once selected.

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- All "administrator" passwords for Trust ICT systems, are kept in a secure place eg school safe and are available upon request by the Executive Principal, Headteachers or Chair of Directors.
- All staff and pupils have a responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The level of security required may vary for staff pupil accounts and the sensitive nature of any data accessed through that account.
- Users should change their passwords whenever there is any indication of possible system or password compromise.
- All staff and pupils have appropriate awareness training on protecting access to their personal username and passwords for ICT access.

Staff Passwords:

- All staff have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- The password should be a minimum of 7 characters long and must include an uppercase character, number, special characters.
- Must not include their names or any other personal information about the user that might be known by others
- The account is "locked out" following six successive incorrect log-on attempts
- Are required to be changed every 90 days
- Should be different for different accounts, to ensure that other systems are not put at risk if one is compromised

Pupil passwords:

- Pupils are taught the importance of password security
- The complexity (ie minimum standards) is set with regards to the cognitive ability of the Pupils.
- Pupils in EYFS and Year 1 have a generic 'class' logon to access school ICT equipment.
- Pupils from Year 2 to Year 4 have a unique, individually-named user account with a generic password suitable to their age.
- Pupils from Year 5 upwards have a unique, individually-named user account and a strong password for access to ICT equipment and information systems available within school.

Internet Filtering and Firewalls

The Trust has a responsibility to ensure that all elements of our schools' infrastructure and network equipment is as safe and secure as possible
To ensure this, all schools within the Trust subscribe to a managed internet filtering and firewall service from Sheffield City Council provided by YHGFL/ICT4C. This service protects the Trust's network infrastructure from external attacks and users from inappropriate content.

Internet filtering

- Each school's internet filtering is set to an appropriate level based on the user accessing the internet.
- The filtering system works on a black and whitelist system which is updated daily from SmoothWall based on the Internet Watch Foundations recommendations.
- Amendments to the black and whitelists are assessed by the Trusts technical team and/or SLT prior to being passed to our provider for implementation.
- Google Safe Search is enforced for all users across all Google services.
- Internet filtering is regularly tested by the technical team for effectiveness and feedback passed to our provider.
- Internet history for users can be requested from the Trust's ISP should the head of school, Executive Principal or Director request it with the help of the technical team.

Firewalls

- By default, firewalls are set to block all inbound traffic other than internet traffic to the Trust's provider's proxy servers.
- The technical team works closely with the council and internet provider to harden servers and vigorously test the firewall should access to servers be needed externally.
- The Trusts ISP provides reverse proxy functionality in the first instance to school webservers to reduce external threats, reducing security only in extreme circumstances once agreed by all parties.
- The firewall is regularly tested by the technical team for effectiveness and feedback passed to the ISP and council.
- Upon a school no longer needing access to a server remotely, the ISP are contacted immediately to remove the firewall rule(s).

Antivirus Protection

All schools within the Trust have antivirus protection across all its end user devices and servers set to an appropriate level of protection to protect the network infrastructure from virus threats. This software is set to scan devices frequently, live scan websites for embedded Trojans and documents upon opening.

Remote Access

The Trust has a number of systems available as online services to encourage teaching and learning beyond the classroom in the form of VLE's, Intranets, Email, Remote Desktop and VPN's. To protect users, Trust data and infrastructure, the following policies are set:

- Automatic disconnections after 15 minutes of inactivity.
- Access to systems based on a least privilege approach and only after being approved by a head of school, Executive Principal or Director.

Users are reminded that when using remote systems they:

- Are aware of their surroundings when using school systems remotely and be aware of who may have sight of my device.
- Ensure their device is not left unattended when signed into school systems. If this is not possible, users ensure they log out and/or lock the device.

Cloud Services

The Trust utilises Cloud Computing services provided by third party providers for many aspects of data storage such as storage of user and Trust data, Email and data backups to increase data availability from multiple devices as well as data security, reducing the risk of loss and theft from unencrypted removable media or theft of devices.

The Trust ensures that all Cloud Computing providers used are on the DFE's approved providers list for education and conforms to the Data Protection Act and the Trust's Data Protection Policy. The Trust ensures that data is stored securely and encrypted, private to the Trust, reliable, is regularly backed up and a disaster recovery procedure is in place.

Staff and pupils primarily use services already provided by the Trust. However, prior to staff and pupils utilising additional Cloud services, they should enquire with the technical team and data controller to ensure that the provider conforms to the above.

Use of Personal Devices (BYOD)

Bring your own device (BYOD) refers to technology models where individuals bring a personally owned device to school for the purpose of teaching or learning.

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by users bringing their own technologies in order to provide a greater freedom of choice and usability. However, the Trust recognise that there are a number of e-safety considerations for BYOD that need to be regularly reviewed. Use of BYOD should not introduce vulnerabilities into existing secure environments.

- Devices should only connect to the advertised BYOD wireless network to ensure a robust filtered internet connection and protect the Trusts network infrastructure.
- Users are fully responsible, at all times, for the personally owned device brought to school.
- Users are responsible for the condition of the device brought to school, including updates, antivirus software, and repair.
- Pupils may only make use of BYOD when given permission by a member of staff or at agreed times of the school day and abide by the schools behaviour policy.

Use of school equipment

Occasional personal use of the school's computers can be beneficial to the development of staff IT skills and to enable staff to maintain a positive work-life balance. However this is at the school's discretion and can be revoked at any time. Any online behaviour and activity by a member of staff whilst using the school systems must be in accordance of the MAT AUA and any policies relating to staff conduct and personal use must not interfere with the member of staff's duties or be for commercial purpose or gain (unless authorised by the SLT).

Management of assets

- Details of all school-owned hardware are recorded in a hardware inventory.
- Details of all school-owned software are recorded in a software inventory.
- All redundant ICT equipment is disposed of through an authorised agency. This includes a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data has the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it is physically destroyed. The school only uses authorised companies who supply a written guarantee that this will happen.
- Disposal of any ICT equipment conforms to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Data Protection

Refer to the Brigantia Learning Trust Data Protection Policy for further information.

Responding to incidents of misuse

It is hoped that all members of the school community are responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The Executive Principal, Headteachers and Safeguarding Officers on each site are informed immediately.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation

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.

Mobile phone usage in schools

It is recommended that staff do not use their own mobile phone devices for communicating with pupils whilst on educational visits or using the camera/video on their mobile phone in class. On occasions when the use of a personal camera is necessary, permission should be sought from the Headteacher/SLT. The images should then be transferred to the school network and deleted from the camera.

Staff use of mobile phones

- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Pupils' use of mobile phones

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Use of Social Media

It is recommended that any contact with pupils and parents only takes place via school approved communication channels e.g. school email address or the school learning platform so it can be monitored and traced in the case of an allegation or concern.

However, the MAT recognises that in some cases there may be pre-existing relationships which mean that any "ban" from adding pupils or parents as friends or contacts on personal social networking sites may be difficult to enforce. It is therefore recommended that members of staff are encouraged to make SLT aware of these exceptions in order to protect themselves from allegations or misinterpreted situations.

It is crucial that all members of staff are made aware of the boundaries and professional practices online in order to protect their professional status. Staff are advised to check their privacy settings on any personal social media sites they use, however they should always remember that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge (even if content is thought to have been deleted or privately shared).

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The schools 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 eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- 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 school 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or VLE
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership

Response to an E-Safeguarding Incident of Concern