Hunter's Bar Infant Online-Safeguarding Policy

December 2018

Policy Introduction

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Scope of the Policy

This policy applies to all members of the school community (including staff, Board of Governors, pupils, volunteers, mothers / fathers / carers, work placement students, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

- **The Education and Inspections Act 2006** empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other Online safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- **The Education Act 2011** gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others. https://www.gov.uk/government/publications/searching-screening-and-confiscation

- The school will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform mothers / fathers / carers of incidents of inappropriate Online safeguarding behaviour that takes place out of school. This includes acting within the boundaries identified in the Department for Education guidance for Searching, Screening and Confiscation.

- **Keeping Children Safe In Education July 2018** This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) (England) Regulations 2011. Schools and colleges must have regard to it when carrying out their duties to safeguard and promote the welfare of children. The document contains information on what schools and colleges **should** do and sets out the legal duties with which schools and colleges **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children 2018**

- **Counter-Terrorism and Security Act 2015** From 1 July 2015 all schools, registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in

the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”.

The statutory guidance on the Prevent duty summarises the requirements on schools and childcare providers in terms of four general themes: risk assessment, working in partnership, staff training and IT policies.

https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

Development / Monitoring / Review of this Policy

This policy has been developed by a working group made up of:

- Headteacher
- Online safety Lead
- Learning Mentor
- Inclusion Lead

Schedule for Development / Monitoring / Review

Title	**(Hunter's Bar Infant) Online safeguarding Policy**
Version	1.0
Date	*December 2018*
Author	*Head teacher*
Approved by the Governing Body on*:*	
Monitoring will take place at regular intervals:	
The Governing Body will notified of any Online safeguarding incidents as appropriate	*Ongoing*
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online safeguarding or incidents that have taken place.	*December 2019*
Should serious Online safeguarding incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity

Communication of the Policy

- The senior leadership team will be responsible for ensuring the school community are aware of the existence and contents of the school Online safeguarding policy and the use of any new technology as and when appropriate.
- The Online safeguarding policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and appropriately communicated to all members of the school community.
- Online safeguarding training/updates will be in place across the school and will include a regular review of the Online safeguarding policy.
- Online safeguarding training will be part of the induction programme for new members of staff
- The Online safeguarding policy will apply when pupils move between education and training providers and will be communicated to all parties accordingly.
- The school approach to Online safeguarding and its policy will be reinforced through the curriculum.
- The key messages contained within the Online safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed Online safeguarding messages across the curriculum whenever the internet or related technologies are used
- Online safety will be introduced to the pupils at the start of each academic year
- Safeguarding posters will be prominently displayed around the setting.

Roles and Responsibilities

We believe that Online safeguarding is the responsibility of the whole school community and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities technology offers in learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Governors

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors CLA Committee* receiving regular information about Online safety incidents and monitoring reports. The role of Safeguarding Governor of the *Governing Body* will include online safety

The role of the Online safety Governor will include:

- regular meetings with the Headteacher
- regular monitoring of Online safety incidents reported by the Head Teacher
- reporting to Resources Committee meeting

Responsibilities of Headteacher and Senior Leaders:

The Headteacher has overall responsibility for safeguarding all members of the school community, though the day to day responsibility for Online safeguarding will be delegated to the Online Safety Co-ordinator

- The Headteacher and senior leadership team are responsible for ensuring that the Online safety Co-ordinator 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 Headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal Online safeguarding role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The Headteacher will receive monitoring reports from the school's IT technician.
- The Headteacher and senior leadership team will ensure that everyone is aware of procedures to be followed in the event of a serious Online safeguarding incident.
- The Headteacher and senior leadership team receive update reports of any incidents from the Online safety Coordinator

Responsibilities of the Safeguarding Team

- To ensure that the school Online safeguarding policy is current and relevant.
- To ensure that the school Online safeguarding policy is systematically reviewed at agreed time intervals.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

Responsibilities of the Online safeguarding Coordinator

- 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 have regular contact with other Online safeguarding committees, e.g. Safeguarding Children Board
- To communicate regularly with school IT technicians.
- To communicate regularly with the senior leadership team.
- 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 local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on Online safeguarding issues to the DSL/DSO and the senior leadership team as appropriate.
- 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 understand, contribute to and promote the school's Online safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- 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 including online exploitation, radicalisation and extremism, bullying, sexting etc.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils and parents should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media 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 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 using only approved and encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff

The school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the Online safeguarding measures, as outlined below. The managed service provider is fully aware of and adhere to the Online safeguarding policy and the acceptable use policies.

- To understand, contribute to and help promote the school's Online safeguarding policies and guidance.
- To understand and adhere to the school staff Acceptable Use Policy.
- To report any Online safeguarding related issues that come to your attention to the Headteacher and Online safeguarding coordinator.
- To develop and maintain an awareness of current Online safeguarding issues, legislation and guidance relevant to their work such as the Prevent Duty.
- To maintain a professional level of conduct in your personal use of technology at all times.
- 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 ICT system.
- To liaise with the senior management team, 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.
- 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, Governors, 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.

When using digital communications, staff, governors and volunteers 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 or parent/carers on social networks. Staff should notify HT of personal friends who are parents if appropriate
- 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, parent/carers 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 or parents/carers (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 Designated Safeguarding Lead (Headteacher)

- To understand the issues surrounding the sharing of personal or sensitive information and to ensure that personal data is protected in accordance with the Data Protection Act 1998.
- To understand the risks and dangers regarding access to inappropriate online contact with adults and strangers.

- To be aware of potential or actual incidents involving the grooming of children and young people in relation to sexual exploitation, radicalisation and extremism.
- To be aware of and understand online bullying and the use of social media and online gaming for this purpose.

Responsibilities of pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To know and understand school policies on the use of digital technologies including mobile phones, digital cameras and any other personal devices ie children are not allowed to have personal digital devices in school.
- 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 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's Online safeguarding policy and the pupil Acceptable Use Policy 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, be aware of what content, websites and Apps they are using, apply appropriate parental controls and ensure they behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology and social media.
- To consult with the school if they have any concerns about their children's use of the internet and digital technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

Going Forwards, to sign a home-school agreement containing the following statements:

- *We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community*
- *We will support the school's Online safeguarding Policy.*
- *Images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet*

- *Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.*
- *Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school*
- *Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances. (see appendices)*

Responsibilities of Other Community/ External Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

- Any external users/organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds.
- The school will ensure that appropriate levels of supervision, filtering and monitoring exist when external users/organisations make use of the internet and ICT equipment within school.

Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a safe and responsible approach. The education of pupils in Online safety is therefore an essential part of the school's Online safety provision. Children and young people need the help and support to recognise and mitigate risks and build their resilience online.

Online safety will be part of a broad and balanced curriculum and staff will reinforce Online safety messages. The Online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. This will be provided in the following ways:

- A planned Online safety curriculum will be provided and should be regularly revisited.
- Key Online safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities, including promoting Safer Internet Day each year.
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- We will discuss, remind or raise relevant Online safety 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 will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- All use will be monitored and they will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of bullying.
- Pupils will be made aware of where to report, seek advice or help if they experience problems when using the internet and related technologies; e.g. mother/father or carer, teacher or trusted staff member, or the CEOP report abuse button.

All Staff (including Governors)

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:

- All staff will receive regular information and Online safeguarding training through a planned programme of annual updates etc.
- All new staff will receive Online safety information and guidance as part of the induction process, ensuring that they fully understand the Online safeguarding policy and Acceptable Use Policies.

- All staff will be made aware of individual responsibilities relating to the Online safeguarding of children and know what to do in the event of misuse of technology by any member of the school community.
- This Online safeguarding policy and its updates will be presented to and discussed by staff in staff training days.
- An audit of the Online safety training needs of all staff will be carried out regularly.
- The Online safety Coordinator will provide advice, guidance and training as required.

Parents/Carers

Mothers / Fathers / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe and responsible way and in promoting the positive use of the internet and social media. Many have only a limited understanding of Online safety risks and issues, yet it is essential they are involved in the Online safety education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may under-estimate 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
- Letters, newsletters, social media
- Parents/Carer coffee mornings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Training – Governors

Governors should take part in Online safety training/awareness sessions, with particular importance for those who are members of the Safeguarding Team. This may be offered in a number of ways:

- Attendance at training provided by the Local Authorty/Learn Sheffield/National Governors Association/other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons)
- Online training

Use of digital and video images

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and pupils instant use of images that they have uploaded themselves or downloaded from the internet. However, everyone needs to be aware of the potential 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. The school will inform and educate users about these risks and their legal responsibilities and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff will inform and educate pupils about the risks and current law associated with the taking, sharing, use, publication and distribution of

images. In particular they should recognise the risks attached to publishing inappropriate images on the internet or distributing through mobile technology.

- Staff are allowed to take digital / video images to support educational aims or promote celebrations and achievements, 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, including mobile phones, 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. Staff will be aware of those pupils where publication of their image may put them at risk.

- Pupils' full names will not be used in association with photographs.

- Written permission from parent/ carers will be obtained before photographs of pupils are published on the school website or social media.

Managing ICT systems and access: Technical infrastructure, equipment, filtering and monitoring

The school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the appropriate Online safety measures and complies with the schools Online safeguarding Policy and Acceptable Use Agreements.

All internal policies and procedures have the appropriate level of visibility within school in an attempt to ensure that they are implemented accordingly. All staff and pupils have completed the appropriate awareness training and where appropriate signed to confirm that they understand the applicable Acceptable Use Policy.

The school 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. It will also need to ensure that the relevant people identified in the previous section will be effective in carrying out their Online safeguarding responsibilities.

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible and meets recommended technical requirements.
- 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 infrastructure and appropriate hardware are protected by active, up to date virus software.
- There will be regular reviews and audits of the safety and security of technical systems.
- The Finance Officer alongside the IT technician provider is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- The administrator passwords for the school ICT system, used by the IT technician provider is also available to the Headteacher senior leader and kept in a secure place.
- All users will have clearly defined access rights to school technical systems and devices.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the staff AUP at all times.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Headtecher or Online safety Coordinator as agreed.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by CBC

- The school's internet provision will include filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content which can be viewed, sent or received through the school's internet provision.
- The school will ensure that the filtering system will block extremist content and protect against radicalisation in compliance with the Prevent Duty, Counter-Terrorism and Security Act 2015
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online safety Lead and Headteacher. All incidents will be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online safety Lead.
- The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the Internet Watch Foundation IWF.
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and Government Prevent block list and this will be kept updated..
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems.
- All information systems require end users to change their password at first log on.
- Users will be prompted to change their passwords at any time that they feel their password may have been compromised.
- Users will be encouraged to have strong, unique passwords
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users 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.
- All staff will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

Management of assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include 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 will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform 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

Personal Data

The Department of Education has published advice and information regarding Cloud software services and the Data Protection Act https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act The Information Commissioners Officer has also published the following guidance https://**ico**.org.uk/.../**cloud computing guidance** for organisations.pdf. Further information is available on the ICO website

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner is the Headteacher who is familiar with information risks and the organisation's response. They have the following responsibilities

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)
- They act as an advocate for information risk management

The Office of Public Sector Information has produced a publication 'Managing Information Risk' to support SIROs in their role.

Information Asset Owner (IAO)

The role of an IAO is to understand

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed of

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The School will:-

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data or their computer is locked when left unattended.

- Transfer data using encryption and secure password protected devices.

- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - the data must be encrypted and password protected
  - the device must be password protected
  - the device must offer approved virus and malware checking software
  - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the SIRO and the applicable IAO.
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

If staff are transmitting sensitive information or personal data e.g. by email or fax it must be transferred by a secure method so it is protected from unauthorised access.

Email

The school does not to use public email accounts for sending and receiving sensitive or personal data.

We do not include personal or sensitive information within the email itself, as the information sent should be by a secure method. This is done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

FAX

- Fax machines will be situated within controlled areas of the school.

- All sensitive information or personal data sent by email or fax will be transferred using a secure method.

- Personal or sensitive information must be within the email itself as the information may be insecure. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

Communication Technologies

	Staff & other adults				Students / 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 school	x							x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones/cameras				x				x
Use of other mobile devices e.g. tablets, gaming devices		x						x
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails				x				x
Use of messaging Apps		x						x
Use of social media		x						x
Use of blogs		x						x

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any agreed channel of digital communication between staff and pupils or parents / carers must be professional in tone and content.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet 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 Radicalisation or extremism in relation to the Counter Terrorism and Security Act 2015					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling					x	
On-line shopping / commerce			x	X		
File sharing			x	X		

Use of social media		x	X		
Use of messaging apps		X	X		
Use of video broadcasting eg Youtube		x	X		

Responding to incidents of misuse

It is hoped that all members of the school community will be 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 or, 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, radicalisation and extremism
- other criminal conduct, activity or materials

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

Any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x	x		X	x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		x	x			x		
Unauthorised downloading or uploading of files		x	x			x		

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		X	X		X			X
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X			X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		X
Using proxy sites or other means to subvert the school's filtering system		X	X		X			X
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		
Deliberately accessing or trying to access offensive or pornographic material		X	X					X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X	X					X

Dealing with Online Complaints

- Parents/Carers are reminded through the Home-School Agreement of appropriate complaints channels and procedures.
- The complaint policy/procedure is clearly detailed on the school website and within the Complaints policy.
- All staff and governors are aware of how to report any negative online comments about the school or members of the school community.
- Staff and governors must under no circumstances reply or react to any online discussion about the school unless prior permission has been granted by the Headteacher.

Response to an Incident of Concern

Contacts

- Safeguarding Advice 0114 205 3535
- Sheffield Police 101
- Local Authority Designated Officer (LADO) 2734850

Online Safety Incident Occurs

If a child is at immediate risk

Inform the Designated Child Protection Coordinator and follow school's child protection procedures

Seek advice from Safeguarding Advisory Service

Contact Sheffield Police (999) urgently if there is immediate danger

Illegal Activity of Material found or suspected

Content

Police 999/101

Report to Internet Watch Foundation (www.iwf.org.uk)

Activity

Child

Staff

Contact safeguarding advice

Child protection procedures and / or criminal action

Contact Local Authority Designated Officer (LADO)

Staff allegations procedures and / or criminal action

Unsure

Consult with SSCB Safeguarding Advisory Desk or E-Safety Project Manager

Inappropriate Activity or Material

Activity

Report to E-safety Lead

Discuss with Headteacher

Child

Possible School Actions:

- Sanctions
- PHSE/citizenship
- Restorative Justice
- Anti Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Seek advice from E-Safety Manager

Content

Staff

Possible School Actions:

- Staff Training
- Disciplinary action
- Involve LADO
- School support e.g. counselling,
- Seek advice from E-Safety Manager

Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for future

Contact Details

Schools Designated Child Protection Officer: Catherine Carr 01142660541
School Online-Safety Coordinator: Claire King 01142660541

Appendices

- Staff and Volunteers Acceptable Usage Policy template
- Parents / Carers Acceptable Usage Policy Agreement template
- Mobile Phone Use
- Links to other organisations, documents and resources
- Legislation

Staff Acceptable Use Policy Guidance

Senior Leadership Teams (SLT) will be encouraging and supporting the positive use of Information and Communication Technology (ICT) to develop curriculum and learning opportunities in schools and settings. Nevertheless it is essential that the use of ICT and online tools is carefully managed to ensure that all members of the school community are kept safe as well as their data and that risks or dangers are recognised and mitigated.

This template Acceptable Use Policy (AUP) provides a structure which is appropriate to the school Online safety ethos and approach. The AUP will need to be adapted by the school for a variety of different audiences and for their individual requirements and systems. It should be developed by a member of SLT and must be approved by the Head Teacher and Governing Body. **It is recommended that staff should be actively involved in writing the AUP to ensure it is appropriate and meets the requirements of the establishment.**

Legislation

Schools may wish to read relevant legislation and information regarding this document and amend the school's AUP accordingly. Schools have a duty of care to safeguard and protect staff under the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999. Key legislation also includes Section 11 of the Children Act 2004 which places a duty on key persons and bodies to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children. Schools may also wish to read and consider the document "Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009), which contains useful guidance around professional use of technology.
www.childrenengland.org.uk/upload/Guidance%20.pdf

Data Protection Act 2018 (GDPR)

Schools must also ensure they comply with the Data Protection Act (DPA) 2018. Under the DPA every organisation that processes personal information (personal data) must notify (register with) the Information Commissioner's Office, unless they are exempt. Specific guidance for education establishments, including information on how to register and check notification may be found here:
http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

The DPA applies to anyone who handles or has access to information concerning individuals and everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. Schools should have a Data Protection and Security Policy in place to outline the legal responsibilities and actions taken to protect personal data in accordance with the DPA. This may include password safety, use of encryption, use of laptops, email and portable data storage devices (e.g. memory sticks) not sharing login information etc. Schools can read more information from the Information Commissioner's Office: http://www.ico.gov.uk/

A Staff AUP is not intended to unduly limit the ways in which members of staff teach or use ICT, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, the reputation of the school is maintained and the safety of all users is ensured. Members of staff are entitled to seek their own legal advice on this matter before signing the AUP.

In order to protect staff members it is essential to have an AUP in place which has been viewed and understood. All employees (including teaching and non-teaching staff) must be aware of the school rules for use of information systems and professional conduct online whether on or off site. Misuse of ICT systems and other professional misconduct rules for employees (whether from Sheffield City Council or other professional bodies) are specific and instances resulting in disciplinary procedures or staff dismissal have occurred.

With internet use becoming more prominent in every day life for personal and professional use, it is important that all members of staff are made aware that their online conduct both in and out of school could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should they be found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. It is therefore important that the AUP is firmly embedded within the school induction process for all members of staff (including any volunteers, part-time staff or work experience placements). It is also important that all members of staff receive up-to-date and relevant training around this issue on a regular basis. All members of staff should read, understand and sign the AUP before being granted access to any of the schools' ICT systems.

Social Media

Some settings may wish to provide more explicit guidance for staff around use of social networking and email as, even when use of social media sites such as Facebook and Twitter occur in their own time using their own computer, it can leave staff vulnerable to abuse or a blurring of professional boundaries.

Schools must be aware they cannot ban staff from using sites in their own personal time; however they can put in place appropriate guidance and boundaries around staff interaction with pupils (past or present) and parents. 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, schools must recognise 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 should be 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). See Social Media Policy for schools for further guidance.

Use of Equipment

Settings may also wish to consider adding a statement regarding their policy on staff using school equipment for personal use. 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 school AUP 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).

Use of Personal Devices

It is recommended that staff do not use their own devices for school business, such as personal mobile phones to communicate with pupils whilst on educational visits or using the camera/video on their mobile phone. 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.

As the school outsources some of its ICT services an AUP has been created as part of the service level agreement and is owned and enforced by both the managed service and the school**.**

The Staff AUP is be reviewed annually and revisited and updated in response to any changes, for example after an incident, introduction of new technologies or after any significant changes to the school organisation or technical infrastructure. Any amendments to the AUP is then be communicated to all staff.

If schools or settings wish to discuss the use and application of Acceptable Use Policies or any other Online safety concerns, please contact the Online safety Project Manager, Sheffield Safeguarding Children Board julia.codman@sheffield.gov.uk 0114 2736945 or contact the Safeguarding Advisory Service 0114 2053554

Further Information

- Sheffield Schools and settings can consult with the Online safety Manager via: julia.codman@sheffield.gov.uk or telephone 0114 2736945.

- Training is available via Safeguarding Training Service on 0114 Telephone: 0114 2735430 or email safeguardingchildrentraining@sheffield.gov.uk

- The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around Online safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.

- "Safer Use of New Technology" is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from www.kenttrustweb.org.uk?esafety

- "Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: http://www.digizen.org/resources/school-staff.aspx

- 360 Degree Safe tool is an online audit tool for schools to review current practice: http://360safe.org.uk/

- "Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009) contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidance%20.pdf

Staff ICT Acceptable Use Policy 2018

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. (See schools GDPR Policy). Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school Online safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead or Deputies and/or the Online safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead or Deputies and/or the Online safety Coordinator.

- I will not attempt to bypass any filtering or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the Headteacher as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.

- I will promote Online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Online safety Coordinator or the Head Teacher.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this

Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood the Staff ICT Acceptable Use Policy.

Signed: ……... Print Name: …… Date: ……

Accepted by: …….. Print Name: ……..

Parent / Carer Acceptable Use Policy Agreement Template

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

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

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

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

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online safety education to help them understand the importance of safe use of ICT – both in and out of school.

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

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will promote positive, safe and responsible behaviour on the internet. I will inform the school if I have concerns over my child's Online safety.

Signed | Date

Use of Photographs, videos and other images within School

Please see Document: The Use of Cameras and Images within Educational Settings and in Social Media

This applies to all staff, volunteers and students on work placement.

There are a number of things that you need to address when using images of people, especially children, some of which is contained in the Data Protection Act 2018:

- You must get the consent of all parents of children appearing in the photograph or video/DVD image before it is created
- You must be clear why and what you'll be using the image for and who will see it
- If you use images from another agency, you need to check that the agency has obtained informed consent

Safeguarding issues:

- Use equipment provided by the school to take the images and not personal devices
- Download and store images in a password protected area of the school network not on personal computers
- When images are stored on the system they should be erased immediately from their initial storage location e.g. camera
- Don't use full names or personal contact details of the subject of any image you use
- Children and families fleeing domestic abuse may be recognised via photos/images and whereabouts revealed to an abusive partner
- No images of a looked after child should be created or used without prior consent from Children's Social Care
- Don't use images of children in swimming costumes or other revealing dress – this reduces the risk of inappropriate use
- Always destroy images once consent has expired or the child has left your school

Consider:

- Are CCTV (security) cameras sited where they may compromise the privacy of individuals?
- How public are your display boards?
- What is the purpose and audience of video's and DVD's you have created?
- Are all of your images and media securely stored at your school?
- Images on websites, and other publicity can become public and outside your control
- Any implications of using images offsite
- The press are exempt from the Data Protection Act, if you invite them to your premises or event, you need to obtain prior consent from parents of children involved
- Including images from different ethnic groups and those of disabled children
- Check out any copyright implications

The Information Commissioner's Office guidance advises that photographs taken for personal use e.g. by parents at special events, at an education setting are not covered by the Data Protection Act.

Useful links/resources:

- **The Use of Cameras and Images within Educational Settings and in Social Media**
- **E-safety section**
  www.safeguardingsheffieldchildren.org.uk
- **Photographs and Videos, Information Commissioners Office, at:**
  http://www.ico.gov.uk/for_the_public/topic_specific_guides/schools/photos.aspx

Mobile phone usage in schools

General issues

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Pupils are not allowed to bring in 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.
- Staff should not use their mobile phones in the classroom. Instead, there are designated safe areas on school where staff can use the mobile phones: staff room, main Reception office, PPA room, Senior Leader offices. However if children are in these areas, mobile phones should not be used, unless in an emergency.
- 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.
- Staff should take no images or videos on mobile phones or personally-owned mobile devices.

Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:

Sheffield Safeguarding Children Board http://www.safeguardingsheffieldchildren.org.uk

Safer Internet Centre: http://www.saferinternet.org.uk/

UK Council for Child Internet Safety: http://www.education.gov.uk/ukccis

CEOP - Think U Know - http://www.thinkuknow.co.uk/

Childnet - http://www.childnet.com

Netsmartz http://www.netsmartz.org/index.aspx

Internet Watch Foundation – report criminal content: http://www.iwf.org.uk/

Guidance for safer working practice for adults that work with children and young people - http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/

Information Commissioners Office/education and ICO guidance on use of photos in schools: www.ico.org.uk

Plymouth Early Years Online safety Toolkit:
http://www.plymouth.gov.uk/early_years_toolkit.pdf
Protecting your personal information online: http://www.ico.org.uk
Getnetwise privacy guidance: http://privacy.getnetwise.org/

Children and Parents

Safer Internet Centre: http://www.saferinternet.org.uk/
CEOP - Think U Know - http://www.thinkuknow.co.uk/
Vodafone Parents Guide: http://parents.vodafone.com/
NSPCC: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone: www.parentinfo.org
Childnet - http://www.childnet.com
Internet Matters: www.internetmatters.org
CBBC – stay safe: http://www.bbc.co.uk/cbbc/

Technology
CEOP Report abuse button: http://www.ceop.police.uk/Safer-By-Design/Report-abuse/
Internet Matters: www.internetmatters.org
Get Safe Online: www.getsafeonline.org

Microsoft Family safety software: http://windows.microsoft.com/en-US/windows-vista/Protecting-your-kids-with-Family-Safety

Legislation

Schools should be aware of the legislative framework under which this Online safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 2018 (GDPR)

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Counter-Terrorism and Security Act 2015

From 1 July 2015 all schools, registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”.
The statutory guidance on the Prevent duty summarises the requirements on schools and childcare providers in terms of four general themes: risk assessment, working in partnership, staff training and IT policies.