Sheffield Springs Academy
The best in everyone™
Part of United Learning

Online Safety Policy 2019/20

Policy Introduction

At Sheffield Springs Academy we believe that technology and the internet can be a wonderful, innovative and educational part of the lives of both young people and the wider community. However we accept that with the

opportunities this presents there will also be risks, this online safety policy aims to decrease these risks wherever possible by educating and raising awareness of how to keep ourselves and others safe online.

Scope of the Policy

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

- **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 academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of academy, but is linked to membership of the academy.

- **The Education Act 2011** gives the academy 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 academy/college 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 safety behaviour that takes place out of academy / college. This includes acting within the boundaries identified in the Department for Education guidance for Searching, Screening and Confiscation.

- **Keeping Children Safe in Education July 2015** this is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent Academy Standards) Regulations 2014 and the Education (Non-Maintained Special Academies) (England) Regulations 2011. Academies 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 academies and colleges **should** do and sets out the legal duties with which academies and colleges **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children 2015**

- **Counter-Terrorism and Security Act 2015** From 1 July 2015 all academies, 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 academies 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 and Review of this Policy

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

- Headteacher – Mark Shipman
- Senior Leadership Team
- Online safety lead – Claire Cartledge
- Staff – including Teachers, Support Staff, Technical staff

Schedule for Development, Monitoring and Review

Title	**Sheffield Springs Academy Online Safety Policy**
Version	1.0

Date	11/04/2017
Author	Claire Cartledge
Approved by the Governing Body on*:*	
Monitoring will take place at regular intervals:	Each term
The Governing Body will receive a report on the implementation of the policy including anonymous details of any online safety incidents at regular intervals:	At the end of each academic year
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 safety or incidents that have taken place. The next anticipated review date will be:	September 2017

Communication of the Policy

- The senior leadership team will be responsible for ensuring the academy community are aware of the existence and contents of the academy online safety policy and the use of any new technology as and when appropriate.
- All amendments will be published and appropriately communicated to all members of the academy community.
- Any amendments will be discussed by the Academy Student Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An online safety training programme will be established across the academy.
- Online safety training will be part of the induction programme for all new staff.
- The online safety policy will apply when pupils/students move between education and training providers and will be communicated to all parties accordingly.
- The academy approach to online safety and its policy will be reinforced through the curriculum.
- We endeavour to embed online safety messages across the curriculum whenever the internet or related technologies are used.
- Safeguarding posters will be prominently displayed around the setting.

Roles and Responsibilities

The Headteacher has overall responsibility for safeguarding all members of the academy community, though the day to day responsibility for online safety will be delegated to the online safety lead.

- The Headteacher and senior leadership team are responsible for ensuring that the online safety lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues 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 academy who carry out the internal online safety role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the online safety lead at least once per term
- The Headteacher and senior leadership team will ensure that everyone is aware of procedures to be followed in the event of a serious online safety incident.
- The Headteacher and senior leadership team receive update reports of any incidents from the online safety lead .

Responsibilities of the Online Safety Lead

- To promote an awareness and commitment to online safety throughout the academy.
- To be the first point of contact in academy on all online safety matters.
- To take day-to-day responsibility for online safety within academy and to have a leading role in establishing and reviewing the academy online safety policies and procedures.
- To communicate regularly with academy technical staff.
- To communicate regularly with the designated governor.
- To communicate regularly with the senior leadership team.
- To create and maintain policies and procedures.
- To ensure that all members of staff receive an appropriate level of training in online safety issues.
- To ensure that online safety education is embedded across the curriculum.
- To ensure that online safety is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.

Responsibilites of the Teaching and Support Staff

- To understand, contribute to and promote the academy's online safety policies and guidance.
- To understand and adhere to the academy staff Acceptable Use Policy.
- To report any suspected misuse or problem to the online safety coordinator.
- To develop and maintain an awareness of current online safety 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 should be on a professional level and only through academy based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.
- To embed online safety 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 safety issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms within the academy.
- 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

- To understand, contribute to and help promote the academy's online safety policies and guidance.
- To understand and adhere to the academy staff Acceptable Use Policy.
- To report any online safety related issues that come to your attention to the online safety coordinator.
- To develop and maintain an awareness of current online safety 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 academy in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the academy 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 academy 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 academy-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within academy.
- 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 academy-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 academy.
- Not share any personal information with a child or young person egg 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.
- 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 academy 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

- 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 Students/ Pupils

- To read, understand and adhere to the academy pupil Acceptable Use Policy.
- To help and support the academy in the creation of online safety policies and practices and to adhere to those the academy creates.
- To know and understand academy policies on the use of digital technologies including mobile phones, digital cameras and any other personal devices.
- To know and understand academy policies on the use of mobile phones in academy.
- To know and understand academy policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in academy 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 academy and at home, including judging the potential risks such as online exploitation, radicalisation, sexting and online bullying.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in academy and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in academy 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 academy.
- To discuss Online safety issues with family and friends in an open and honest way.

Responsibilies of Parents/ Carers

- To help and support the academy in promoting online safety.
- To read, understand and promote the academy's online safety 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 academy 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 safety 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 academy if they have any concerns about their children's use of the internet and digital technology.
- To agree to and sign the home-academy agreement which clearly sets out the use of photographic and video images outside of academy.

Responsibilities of other Community/ External Users

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

Education

Students/ 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 students / pupils in e-safety is therefore an essential part of the academy's e-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 e-safety curriculum will be provided as part of Computing and ACE Day provision and other lessons and should be regularly revisited.
- Key online safety messages will be reinforced as part of a planned programme of assemblies, including promoting Safer Internet Day each year.
- Students 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.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- 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.
- Students / Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind students / pupils about their responsibilities through an end-user Acceptable Use Policy which they will sign/will be displayed throughout the academy/college and will be displayed when a user logs on to the network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Heldesk can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and should be submitted through the normal ticketing procedure.
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students / 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.
- Students will be taught about the impact of online bullying and know how to seek help if they are affected by any form of bullying.
- Students will be made aware of where to report, seek advice or help if they experience problems when using the internet and related technologies.

All Staff (including Governors)

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

- All staff will receive regular information and online safety training through a planned programme of termly staff briefings
- All new staff will receive online safety information and guidance as part of the induction process, ensuring that they fully understand the online safety policy and Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the online safety of children and know what to do in the event of misuse of technology by any member of the academy community.
- An audit of the online safety training needs of all staff will be carried out regularly.
- The online safety lead 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 e-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 online 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 academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and students 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 academy 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 students / 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 academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment, the personal equipment, including mobile phones, of staff should not be used for such purposes.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. Staff will be aware of those students where publication of their image may put them at risk.
- Students' full names will not be used in association with photographs.
- Student's work can only be published with the permission of the student and mother / father or carers.

Filtering Internet Access

As all academies will be aware, the internet is a valuable tool for teaching and learning. Unfortunately, not all content that is available on the internet is appropriate so provision has to be made to ensure that a suitable, fit-for-purpose internet filtering solution is deployed. As with any aspect of education, decisions and guidance from OFSTED very much influence what academies need and want. The OFSTED report, 'Safe use of new technologies' (February 2010) had, as one of its key findings;

'Pupils in the academies that had 'managed' systems had better knowledge and understanding of how to stay safe than those in academies with 'locked down' systems. Pupils were more vulnerable overall when academies used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.'

- The academy uses a filtered internet service. The filtering system is provided by
- The academy's internet provision will include filtering appropriate to the age and maturity of pupils.
- The academy will always be proactive regarding the nature of content which can be viewed, sent or received through the academy's internet provision.
- The academy 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 academy 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 E-safety Lead. All incidents will be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the E-safety Lead.

- The academy will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the Internet Watch Foundation IWF.
- The academy will regularly review the filtering product for its effectiveness.
- The academy 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 academy 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-academy requirement across the curriculum.

Data Protection

Personal Data

The academy may have access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children / young people, members of staff / volunteers / students and mothers and fathers / carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by mothers and fathers / carers or by other agencies working with families

The Data Protection Act 1998 requires every organisation processing personal data to notify with the Information Commissioner's Office, unless they are exempt.

Settings that work with children and young people are likely to be under greater scrutiny in their care and use of personal data, following high profile incidents. In April 2010 the Information Commissioners Office introduced a new maximum £500K fine for breaches of information security for both public and private sector organisations.

All academies must understand the implications of not securing the information assets they hold and should look to appoint a Senior Information Risk Officer (SIRO) This role may well be combined with the academies Data Protection Officer and, where appropriate, Information Asset Owners (IAO).

Cloud Computing

Academies that use cloud hosting services may be required to seek parental permission to set up an account for pupils/students. Cloud systems such as Google Apps for Education services may require that academies obtain 'verifiable parental consent' for children to be able to use the system and services.

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 should be a member of the senior leadership team (normally 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

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 Academy 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 academy policy once it has been transferred or its use is complete.
- The academy has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within academy.
- The academy has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the academy 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 academy 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 academy 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 academy.
- 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 academy's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

If you 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

It is advisable not to use public email accounts for sending and receiving sensitive or personal data.

DO NOT include personal or sensitive information within the email itself, as the information sent should be by a secure method. 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.

Encryption makes a file non readable to anyone who does not have the password to open it, therefore, it reduces the risk of unauthorised people having access to the information and protects staff from breaching the law.

Fax

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

Passwords

A secure and robust username and password convention exists for all system access (email, network access, academy management information system).

Students all key stages will have a unique, individually-named user account and password for access to ICT equipment and information systems available within the academy.

All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within the academy.

All information systems require end users to change their password at first log on.
Users should be prompted to change their password at prearranged intervals or at any time that they feel their password may have been compromised.

Users should change their passwords whenever there is any indication of possible system or password compromise.

All staff and students have a responsibility for the security of their usernames and passwords. 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.

The academy will enforce specific sanctions to any end user (staff or student) for attempting to hack other user accounts.

All staff and students will have appropriate awareness training on protecting access to their personal usernames and passwords for ICT access.

All staff and students will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to usernames 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 log on. Do not include
- Passwords in any automated logon procedures.
- Never save system-based usernames and passwords within an internet browser.

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in the academy is allowed.

All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within the academy to ensure that any risks are managed to an acceptable level. Emerging technologies can incorporate software and/or hardware products.

The Academy will periodically review which technologies are available within the academy for any security vulnerabilities that may have been discovered since deployment. All new technologies deployed within the academy will be documented within the online safety and acceptable use of any new or emerging technologies in use within the academy will be reflected within the academy online safety and Acceptable Use Policies.

Prior to deploying any new technologies within the academy, staff and students will have appropriate awareness training regarding safe usage and any associated risks. The academy will audit ICT equipment usage to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities. Methods to identify, assess and minimise risks will be reviewed regularly. A BYOD policy will be established by September 2017.

Any use of personal devices on the academy network will be clearly detailed within the personal device/**BYOD policy.**

Email Usage

Staff will be reminded when using email about the need to send polite and responsible messages.

Students will be reminded about the dangers of revealing personal information within email conversations. Students must not reveal personal details of themselves or others in email communications. Students should get prior permission from an adult if they arrange to meet with anyone through an email conversation.

Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.

Students and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments. All email and email attachments will be scanned for malicious content. Students and staff should never open attachments from an untrusted source but should consult the network manager first.

Communication between staff and students or members of the wider academy community should be professional and related to academy matters only.

All students with active email accounts are expected to adhere to the generally accepted rules of netiquette; particularly in relation to the use of appropriate language. They should not reveal any personal details about themselves or others in email communication or arrange to meet anyone without specific permission.
Any inappropriate use of the academy email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.All email users within academy should report any inappropriate or offensive emails through the incident-reporting mechanism within the academy.

Sanctions will be in place for any user (student or staff) who hacks into another user's email account.
Students must immediately tell a designated member of staff if they receive any inappropriate or offensive email. Students must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.

Irrespective of how students or staff access their academy email (from home or within the academy), academy policies still apply.

Emails sent to external organisations should be written carefully and authorised before sending to protect the member of staff sending the email.

Chain messages will not be permitted or forwarded on to other academy-owned email addresses.

All emails should be written and checked carefully before sending, in the same way as a letter written on academy-headed paper.

Staff who send emails to external organisations, parents or students, are advised to carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.

All emails that are no longer required or of any value should be deleted.

Email accounts should be checked regularly for new correspondence.

When away for extended periods, 'out-of-office' notification should be activated so that colleagues are aware that you are not currently available.

Social Media

As an academy we recognise that teachers and support staff are individuals with the right to private lives. Off-duty conduct may however still a bearing have on the professional life of a teacher/ member of staff.

Inappropriate use of social media by a student or a member of staff can have significant implications on their careers, future careers and personal lives and should therefore be used with caution and thorough understanding. Sound judgement and due care should therefore be exercised at all times.

Throughout this policy any site or application where contact can be made and shared with others is considered to be social media.

The following types of misuse will be subject to immediate disciplinary action:

- inappropriate electronic communication with pupils, colleagues and
- parents/carers, including SMS and instant messaging;
- posting/sending sexually explicit pictures/images to colleagues or pupils;
- grooming - whereby a teacher uses electronic messages with a view to establishing an inappropriate relationship with a pupil;
- possessing, making, viewing or distributing indecent images of children;
- using inappropriate YouTube content in the educational setting.

How can teachers minimise risk when using electronic communication and social networking:

- Always maintain a formal and courteous and professional tone in communicating with pupils and ensure that professional boundaries are maintained.
- You should not identify yourself as an employee of the academy within any personal social media accounts.
- Only use official channels of communication e.g. work e-mail addresses.
- Do not exchange private texts, phone numbers, personal e-mail addresses or photos of a personal nature with pupils.
- You must decline student-initiated 'friend' requests from pupils and do not instigate any yourself.
- It is inappropriate to have ex-pupils as friends on social media within five years of them leaving the academy.
- It is also necessary to decline contact invitations from parents/ carers and remind parents of more formal channels through which they can discuss their child's education.
- Operate online in a way in which would not call into question your position as a professional - a good rule to follow is that if you wouldn't do or say something in real-life then don't do it online.
- Teachers and support staff should realise that pupils will naturally be curious about your personal life outside school and may try to find out more about you, it is therefore necessary in this digital age to minimise and manage risks online.
- You should manage your privacy settings and keep them under review. These are particularly important in regard to photos.
- Remember that no privacy mechanism is 100% guaranteed.
- Ensure your settings prohibit others from tagging you in any photos or updates without your permission. You can ask others to remove any undesirable content related to you.
- Always consider that conversations held online may not be private. Be aware of who may have access to what you post, for example members of groups can often see fellow members' posts.
- Do not discuss pupils, colleagues, parents or carers online or criticise your employer or others within the school community, respect pupil privacy at all times.

- Use strong passwords and change them regularly. Protect your mobile phone/smart phone/tablet computer with a PIN, especially when in school, to protect access to its content and potential misuse. The online safety lead can offer advice on this if necessary.
- You should immediately bring the matter to the attention of the headteacher if you are the victim of cyber bullying or are uncomfortable with comments, photos or posts made by pupils about you.
- Teachers and support staff are encouraged to regularly search for their online presence and check what is publically available to be viewed via Google, Bing and other search engines.

Discovery of Inappropriate Material

If staff/ students have been made aware of inappropriate images of a child or young person, they should inform the designated Child Protection Officer (CPO) in school, as the protection of the child or young person is a paramount.

The school's police liaison officer should also be informed at this stage, and he/ she will be able to give more specific advice about the legalities of the situation and removal of the image.

The image should not be deleted until local police have agreed to it. If the image has been uploaded to any website or social networking site, the school will contact the provider of the service to have it removed.

The parents of the young person should be notified of the situation. The school may consider in-house counselling for the young people concerned, particularly if they were depicted in the image.

The school will run termly classes or assemblies to highlight the issue of sexting and encourage young people to practice safe and responsible behaviour in their online activity.

Unsuitable/ Inappropriate Activities

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

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

proposals or comments that contain or relate to:	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 academy or brings the academy into disrepute				X	
Using academy systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy / 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)						
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce			X			
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting eg Youtube					X	

Responding to Incidents of Misuse

It is hoped that all members of the academy 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

Dealing with Online Complaints

The nature of the internet, and the two-way communication that it brings, means that many parents will now turn to the online world to air their concerns or grievances. Academies often find that a seemingly minor incident can escalate quite quickly with Facebook pages or groups being formed where parents can discuss issues and gather support. It is advised that there should be a procedure for dealing with online complaints, particularly in relation to derogatory comments made in social networks by parents/carers or other members of the academy community.

Managing your academy digital footprint is as crucial as managing a personal one. This is equally important for academies that have a social-media presence as well as those with just a website. Staff must understand the importance of not being drawn into discussions or reacting to complaints. It is vital that all staff, governors, pupils and parents are aware that official complaints channels exist and that the internet is not a recognised option.

Key Steps:

- Ensure that all staff and governors are aware of how to report and react to negative online statements
- Review your Acceptable Use Policies to ensure that they clearly state that staff and governors must not be drawn in to any online discussions.
- Review and update your complaints procedure to include reference to not utilise online channels for complaints.

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

Management of Assests

Details of all Academy-owned hardware will be recorded in a hardware inventory.

Details of all Academy-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 Academy 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.

Response to an Incident of Concern