Woodlands Academy
E safety Policy 2020-2021

We give our learners the skills and knowledge

to embrace the digital world safely and securely.

E-Safety and Internet Policy
Woodlands Academy 2020-2021

Aims and Ethos:

- To set out the key principles expected of all members of the Academy community at Woodlands Academy with respect to the use of ICT-based technologies.

- To safeguard and protect the children and staff of Woodlands Academy.

- To assist Academy staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.

- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.

- To have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other Academy policies.

- To ensure that all members of the Academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

- To minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our Academy community can be summarised as follows:

Content -	Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse Lifestyle websites, for example pro-anorexia/self-harm/suicide sites, Hate sites Content validation: how to check authenticity and accuracy of online content
Contact	Grooming, Cyber-bullying in all forms Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
Conduct	Privacy issues, including disclosure of personal information Digital footprint and online reputation Health and well-being (amount of time spent online (Internet or gaming)) Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) Copyright - little care or consideration for intellectual property and ownership – such as music and film (Ref Ofsted 2013)

Scope

This policy applies to all members of Woodlands Academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Academy ICT systems, both in and out of Woodlands 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 is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the Academy, but is linked to membership of the Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Safeguarding Ethos - The safety and wellbeing of our pupils is of paramount importance

Woodlands Academy and the Raleigh Learning Trust is committed to safeguarding and promoting the welfare of children and young people, and we expect all staff and volunteers to share this commitment.

This Academy aims to create and maintain a safe environment for all members of staff and pupils

- We will manage situations should child welfare concerns arise
- We aim to create an atmosphere of trust in which pupils feel confident to confide any concerns
- We will help young people to understand the difference between acceptable and non - acceptable behaviour
- We will teach pupils to stay safe from harm

Roles and Responsibilities with the Academy

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the Academy uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the ICT (E-Safety) Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

ICT (E-Safety) Co-ordinator / Designated Child Protection Lead (DSL)	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy e-safety policies / documents
	• Promotes an awareness and commitment to e-safeguarding throughout the Academy community
	• Ensures that e-safety education is embedded across the curriculum
	• Liaises with Academy ICT technical staff
	• To communicate regularly with SMT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies where necessary
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Governors / E-safety governor	• To ensure that the Academy follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of safeguarding / E-Safety Governor • To support the Academy in encouraging parents and the wider community to become engaged in e-safety activities • The role of the safeguarding / E-Safety Governor will include: • regular review with the E-Safety Co-ordinator (including e-safety incident logs, filtering / change control logs)

Role	Key Responsibilities
IT technician (schools IT)	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the Academy's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the Academy ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on Academy-owned devices • The Academy's policy on web filtering is applied and updated on a regular basis • That he / she keeps up to date with the Academy's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the Academy's e-security and technical procedures
Teachers	• To embed e-safety issues in all aspects of the curriculum and other Academy activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended Academy activities if relevant) • 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
All staff	• To read, understand and help promote the Academy's e-safety policies and guidance • To read, understand, sign and adhere to the Academy staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current Academy policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional 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 etc.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: it is expected that parents / carers would sign on behalf of the pupils if necessary) • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand Academy policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand Academy policy on the taking / use of images and on cyber-bullying.

Role	Key Responsibilities
	• To understand the importance of adopting good e-safety practice when using digital technologies out of Academy and realise that the Academy's E-Safety Policy covers their actions out of Academy, if related to their membership of the Academy • 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 help the Academy in the creation/ review of e-safety policies
Parents/ carers	• To support the Academy in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the Academy's use of photographic and video images • To read, understand and promote the Academy Pupil Acceptable Use Agreement with their children • To access the Academy website on-line student in accordance with the relevant Academy Acceptable Use Agreement. • To consult with the Academy if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within Academy

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the Academy website/staffroom/ classrooms
- Policy to be part of Academy induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole Academy community, usually on entry to the Academy
- Acceptable use agreements to be held in common files for all pupils and staff members

Handling complaints:

The Academy will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a Academy computer or mobile device. The Academy cannot accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview/counselling by the class tutor / E-Safety Coordinator / Headteacher;
  - Informing parents or carers;
  - The removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - Referral to LA / Police.

- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with Academy / LEA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other Academy policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the Academy Development Plan and Behaviour policy

The Academy has an e-safety coordinator who will be responsible for document ownership, review and updates.

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the Academy
- The e-safety policy has been written by the Academy e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SMT and approved by Governors and other stakeholders. All amendments to the Academy e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-safety curriculum

This Academy

- Has a clear, progressive e-safety education programme as part of the ICT and Computing curriculum & PSHE curriculum. It is built on safeguarding and national guidance.

  This covers a range of skills and behaviours appropriate to their age and experience, including:

  - To STOP and THINK before they CLICK
  - To develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - To know how to narrow down or refine a search;
  - [for older pupils] To understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - To understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
  - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;

  - To understand why they must not post pictures or videos of others without their permission;
  - To know not to download any files – such as music files - without permission;
  - To have strategies for dealing with receipt of inappropriate materials;
  - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
  - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
  - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the Academy/will be displayed when a student logs on to the Academy network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff Training

This Academy

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the Academy's e-safety education program annual updates
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the Academy's Acceptable Use Policies.

Parent awareness and training

This Academy

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in Academy newsletters; on the Academy web site;
  - demonstrations, practical sessions held at Academy;

- suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this Academy, all users:

- Are responsible for using the Academy ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to Academy systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- All pupils need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- All pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- All pupils should understand the importance of adopting good e-safety practice when using digital technologies out of Academy and realise that the Academy's E-Safety Policy covers their actions out of Academy, if related to their membership of the Academy
- Will be expected to know and understand Academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Academy policies on the taking / use of images and on cyber-bullying

Staff

- Are responsible for reading the Academy's e-safety policy and using the Academy ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the Academy
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this Academy:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the Academy's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues

- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the Academy. The records are reviewed/audited and reported to the Academy's senior leaders, Governors /the LEA
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

- Internet access, security (virus protection) and filtering

This Academy:

- Has the educational filtered secure broadband connectivity through the Nottingham City School's IT Dept.
- Ensures network healthy through use of anti-virus software etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE or LEA approved systems, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Works in partnership with the LEA to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the ICT Coordinator or system administrator(s) logs or escalates as appropriate
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LEA.

- Network management (user access, backup)

  This Academy
  - Uses individual, audited log-ins for all users
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
  - Ensures the Systems Administrator (Schools IT dept) is up-to-date with services and policies and requires the Technical Support Provider to be up-to-date with services and policies;
  - Storage of all data within the Academy will conform to the UK data protection requirements

    Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this Academy:

- Ensures staff read and sign that they have understood the Academy's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- We provide pupils with an individual network log-in username. They are also expected to use a password;
- All pupils have their own unique username and a password which gives them access to the Internet and the shared resources
- *For some older pupils, (with parental permission) their own Academy approved email account*;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Has set-up the network so that users cannot download executable files / programmes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the Academy provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the Academy, is used solely to support their professional responsibilities and that they notify the Academy of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. equipment installed and checked by approved Suppliers / LEA electrical engineers
- Ensures that access to the Academy's network resources from remote locations by staff is restricted and access is only through Academy / LEA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- All computer equipment is installed professionally and meets health and safety standards;
- Reviews the Academy ICT systems regularly with regard to health and safety and security.

Password policy

- This Academy makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access Academy systems. Staff are responsible for keeping their password private.

E-mail

This Academy

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the Academy website. We use anonymous or group e-mail addresses, for example headteacher@woodlands.nottingham.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class)
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of provided technologies to help protect users and systems in the Academy, including desktop anti-virus software, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Pupils can only receive external mail from, and send external mail to, addresses if the Safe Mail rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in Academy and at home i.e. they are taught:
    - Pupils should not to give out their e-mail address unless it is part of a Academy managed project or to someone they know and trust and is approved by their teacher or parent/carer;

- Pupils should know that an e-mail is a form of publishing where the message should be clear, short and concise;
- Pupils should know that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper;
- Pupils should know they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- Pupils should know to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- Pupils should know that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- Pupils should know that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- Pupils should know not to respond to malicious or threatening messages;
- Pupils should know not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- Pupils should know not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- Pupils should know that forwarding 'chain' e-mail letters is not permitted.

- Pupils sign the Academy Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with, on an annual basis.

Staff:

- Staff only use e-mail systems for professional purposes
- Access in Academy to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. We use secure, LEA / DfE approved systems.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on Academy headed paper. That it should follow the Academy 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;

- All staff sign our Academy Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Academy website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The Academy web site complies with the statutory DfE guidelines for publications;
- Most material is the Academy's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

- The point of contact on the web site is the Academy address, telephone number and we use a general email contact address, e.g admin@woodlands.nottingham.sch.uk Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the Academy website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' Academy approved blogs or wikis to password protect them and run from the Academy website.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the Academy's preferred system for such communications.
- The Academy's preferred system for social networking will be maintained in adherence with the communications policy.

Academy staff will ensure that in private use:

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

Video Conferencing

- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.
- We only use approved or checked webcam sites; such as Skype

5. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into Academy are entirely at the staff member, students & parents' or visitors own risk. The Academy accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into Academy.
- Student mobile phones which are brought into Academy must be turned off (not placed on silent) and given to members of staff on arrival at Academy. They must remain turned off and out of sight until the end of the day. Staff members may only use their phones during Academy break times. All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any mobile phone is not allowed; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The Academy reserves the right to search the content of any mobile or handheld devices on the Academy premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the Academy day, they should do so only through the Academy's telephone. Staff may use their phones during lessons and break times only for matters relating to the Academy and not for personal use.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal Academy time. They should be switched silent at all times.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the Academy site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal Academy time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar 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.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All mobile phones and personally-owned devices will be handed in should they be brought into Academy.

Students' use of personal devices

- The Academy strongly advises that student mobile phones should not be brought into Academy.
- Pupils that do bring mobile phones in will have to hand them into staff on point of entry to Academy or to their class tutor.
- The Academy accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the Academy policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released to parents or carers in accordance with the Academy policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a Academy phone. Parents are advised not to contact their child via their mobile phone during the Academy day, but to contact the Academy office.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with an Academy phone where contact with students, parents or carers are required.
- Mobile Phones and personally-owned devices will be switched to 'silent' mode or off. Unless they are required to be able to contact the on call system or SMT.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior Management Team. For example on a school trip.
- Staff should not use mobile devices for personal reasons unless in an emergency. Texting, emails and phone calls of a personal nature are not allowed during lessons (except in emergency situations)
- Personally-owned devices, such as mobile phones or cameras, cannot be used to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the Academy policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for Academy duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a Academy mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a Academy-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In this Academy:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the Academy agreement form when their daughter / son joins the Academy and annually thereafter.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published Academy produced video materials / DVDs;
- If specific pupil photos (not group photos) are used on the Academy web site, in the prospectus or in other high profile publications the Academy will obtain individual parental or pupil permission for its long term use
- The Academy blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or Academy. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

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 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 equipment that may have held personal data will have the storage media forensically wiped. 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.

6. Grooming and sexual exploitation

Definition

Sexual exploitation is a form of abuse whereby children are deliberately persuaded to enter into situations where they receive something (for example, gifts, money, food, accommodation) in exchange for sexual activity. Most victims are female, though there is thought to be considerable underreporting by male victims, who may be confused about their sexuality and be unwilling to draw attention to themselves. Most perpetrators are male, though women may also be involved. Children may be exploited by an individual, several individuals working as an organised group, or by a gang.

Grooming is the process of 'preparing' a boy or girl for a sexual purpose. Grooming is often slow and subtle, continuing for several weeks or months and lulling the child into a false sense of security. It always involves manipulation and deceit.

Two types of grooming are recognised: street grooming which occurs in the community, and online grooming using technology including the internet and mobile phones.
(Note: references to children, young people or pupils mean all individuals under the age of 18. References to parents mean parents, carers and others with parental responsibility.)

The complexity and challenge posed by grooming and sexual exploitation

It can be difficult to identify children and young people who are at risk of sexual exploitation. The grooming process draws children in to what they initially perceive as a new and caring relationship with an exciting older boyfriend or girlfriend.

Attempts to explain the risks to the child may be met with derision and hostility. By the time the child realises the reality of the 'relationship' they may have been seriously sexually and physically abused,

threatened with the distribution of indecent photographs or videos of their abuse and warned that they will put themselves or their family in danger if they speak out. Unsurprisingly, the child may be reticent to disclose their abuse, particularly to people in positions of authority such as teachers, social workers or police officers. The child may find it impossible, for a number of reasons, to speak to their parent and their abusers will have sought to isolate them from their family and friends. Some children may have developed drug or alcohol addictions and rely on their abusers for supply.

A fundamental learning point to emerge from cases of sexual exploitation such as those in Rotherham, Derby, Rochdale and Oxford and the Jimmy Saville case is that many children who try to disclose their abuse are not believed, or value judgements are made by professionals about the young person, suggesting they are 'willing partners' in a lifestyle they have 'chosen'. Remarkably, some young people's concerns and disclosures have been dismissed as groundless because of their challenging behaviour, involvement in crime or history of going missing from home, school or care.
As an Academy we have a responsibility to do all we can to raise awareness of sexual exploitation and grooming and to identify and support any pupil who is at risk of abuse.

Action by School

Academy staff are the only professionals in daily direct contact with children and we play an important role in keeping pupils' safe and supporting them when things go wrong. To help keep our pupils safe from sexual exploitation and grooming we will:
- Promote healthy and safe relationships
- Raise pupils' awareness of sexual exploitation and grooming at an age appropriate level
- Raise staff awareness of sexual exploitation and grooming
- Help parents to understand the issues
- Contribute to multi-agency safeguarding and child protection arrangements

The legal framework

Sections 175 and 157 of The Education Act 2002 require the governing bodies of all schools and colleges and the proprietors of independent schools to safeguard and promote the welfare of pupils.

The statutory child protection guidance for schools is Safeguarding Children and Safer Recruitment. This guidance was replaced by Keeping Children Safe in School in 2015. The new advice document explains the role of the school.

'It is important that children receive the right help at the right time. For that to happen, everyone who comes in contact with children in school has a role to play in identifying concerns early, sharing information and taking prompt, informed action. Therefore all professionals in schools should be vigilant and act quickly when they suspect a child is suffering, or is likely to suffer, harm.'

The multi-agency child protection guidance Working Together to Safeguard Children (2013) emphasises that:
'… professionals working in universal services have a responsibility to identify the symptoms and triggers of abuse and neglect, to share that information and work together to provide children and young people with the help they need. Practitioners need to continue to develop their knowledge and skills in this area. They should have access to training to identify and respond early to abuse and neglect, and to the latest research'
The Sexual Offences Act 2003 covers sexual offences against children, including offences involving grooming and the internet and trafficking.

Procedures to follow

Early identification of risk is known to be a crucial factor in reducing harm so the vigilance of school staff is critically important. Staff should not attempt to manage concerns about sexual exploitation or grooming in isolation.

The DSL must always be informed and school leadership will enlist the advice and support of children's social care and the police as appropriate.

7. Cyberbullying

For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

The Academy recognises that both staff and students may experience cyber bullying and will commit to preventing any instances that should occur. We regularly educate staff, students and parents on the importance of staying safe online, as well as being considerate to what they post online.

The Academy will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students. We have a zero tolerance policy for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

The DSL, Head of school and ICT coordinator will decide whether it is appropriate to notify the police or the Director at the LA of the action taken against a student.

8. Radicalisation

The role of the Academy

We recognise our duty to ensure that through our Academy vision, values, rules, diverse curriculum and teaching we promote tolerance and respect for all cultures, faiths and lifestyles.

The governing body also ensures that this ethos is reflected and implemented effectively in academy policy and practice and that there are effective risk assessments in place to safeguard and promote students' welfare.

We have a duty to prepare our children for life in modern Britain and to keep them safe. Pupils who attend our school have the right to learn in safety.

We do not tolerate bullying of any kind and will challenge derogatory language and behaviour towards others. All staff are expected to uphold and promote the fundamental principles of British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs.

Government strategies

The Office for Security & Counter Terrorism works to counter the threat from terrorism and their work is detailed in the counter terrorism strategy CONTEST.

This strategy is based on four areas of work:

- Pursue - To stop terrorist attacks
- Prevent - To stop people becoming terrorists or supporting terrorism
- Protect - To strengthen our protection against a terrorist attack
- Prepare - To mitigate the impact of a terrorist attack

Radicalisation online

The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages.

The filtering systems used in the Academy blocks inappropriate content, including extremist content and monitors for extremist activity, alerting leadership if it occurs. We also filter out social media, such as Facebook. Searches and web addresses are monitored and the ICT technician will alert senior staff where there are concerns and prevent further access when new sites that are unblocked are found.

Where staff, children or visitors find unblocked extremist content they must report it to the ICT coordinator and the DSL immediately.

We are aware that children and young people have access to unfiltered internet when using their mobile phones and staff are alert to the need for vigilance when pupils are using their phones.
The Acceptable Use of ICT Policy refers to preventing access to extremist content. Pupils and staff are asked to sign the Acceptable Use of ICT Policy annually to confirm they have understood what is acceptable. Pupils and staff know how to report internet content that is inappropriate or of concern.

The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content. But no filtering system is perfect and so staff have to be constantly vigilant so that offensive material cannot be viewed in school at any time.

Procedures for referring concerns

Although serious incidents involving radicalisation have not occurred within the Raleigh Learning Trust to date, it is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach.

Staff are reminded to suspend any professional belief that instances of radicalisation ‘could not happen here’ and to refer any concerns through the appropriate channels (currently via the DSL or Child Protection/ Safeguarding Coordinator).

When there are significant concerns about a pupil the Designated Safeguarding Lead in liaison with the head of school. Please refer to the safeguarding policy, which should be read in conjunction with this section on radicalisation.

Searching, Screening and Confiscation Guidance Update

Staff may lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Any data, files or images that are not believed to be unlawful, may be deleted or kept as evidence of a breach of the school's behaviour policy.

Woodlands Academy Senior Leadership Team need to be alerted to any concerns regarding electronic devices. 2 members of the leadership team will search the electronic device and take the appropriate action.

Staff reporting a concern of this nature must inform the behaviour lead immediately and an incident form completed.

If there is a concern regarding the material on the electronic device a concern form must be completed and handed to the DSL by the end of the working Day. The DSL will take the appropriate action according to the material discovered by SLT.