Woodkirk Academy
&
The Sixth Form @ Woodkirk Academy

ONLINE SAFETY POLICY

Woodkirk Academy is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers and visitors to share this commitment. We are fully committed to ensuring that consistent effective safeguarding procedures are in place to support children, families and staff at school.

Reviewed and approved by the Local Governing Board on 5 October 2021

A MEMBER OF
Leodis Academies Trust

CONTENTS

1. STATEMENT OF INTENT

1.1. Woodkirk Academy understands that using online services is an important aspect of raising educational standards, promoting student achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of students and staff.

1.2. The breadth of issues classified within Online Safety is considerable, but they can be categorised into four areas of risk:

1.2.1. Content
Being exposed to illegal, inappropriate or harmful material, for example pornography, fake news, self-harm and suicide and discriminatory or extremist views.

1.2.2. Contact
Being subjected to harmful online interaction with other users, for example peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit children.

1.2.3. Conduct
Personal online behaviour that increases the likelihood of, or causes, harm, for example sending and receiving explicit messages and cyberbullying.

1.2.4. Commerce
Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

1.3. The measures implemented to protect students and staff revolve around these areas of risk. Woodkirk Academy has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

2. INTRODUCTION

2.1. This policy recognises the commitment of Woodkirk Academy to Online Safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep students safe when using technology. We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks while continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with students.

2.2. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (**"AUP"**) which we expect all staff and students to follow.

2.3. As part of our commitment to Online Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

2.4. Woodkirk Academy staff have a responsibility in accordance with the latest 'Keeping Children Safe in Education (DfE) to safeguard students and report abuse immediately to Designated Staff in accordance with the Academy's Safeguarding & Child Protection Policy. All staff will attend

child protection training which outlines forms of abuse, and includes the indicators and signs of CSE, radicalisation and peer on peer abuse.

3. SCOPE OF THE POLICY

3.1. This policy applies to the whole school community including the senior leadership team, **("SLT"**) school board of governors, all staff employed directly or indirectly by Woodkirk Academy, visitors and all students.

3.2. The SLT and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for Online Safety within school will be reflected within this policy.

3.3. The Education and Inspections Act 2006 empowers principals, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other Online Safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

3.4. The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Principal believes it contains any material that could be used to bully or harass others.

3.5. This guidance takes into account the following:

3.5.1. Safeguarding Children in Digital World (DfE);
3.5.2. CEOP (Child Exploitation and Online Protection);
3.5.3. Communication Act 2003 (Section 27 – Improper Use of Public and Electronic Communications Network);
3.5.4. Data Protection Act 2018;
3.5.5. Harmful online challenges and online hoaxes (DfE 2021);
3.5.6. Keeping Children Safe in Education (DfE 2021);
3.5.7. Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes; advice for educational settings working with children and young people';
3.5.8. Teaching Online Safety in School (DfE 2019); and
3.5.9. Searching, Screen and Confiscation (DfE 2018).

3.6. The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate Online Safety behaviour that takes place out of school.

3.7. This document has links to the following:

3.7.1. Woodkirk Academy Anti-bullying and Harrassment Policy;
3.7.2. Woodkirk Academy Safeguarding & Child Protection Policy;
3.7.3. Woodkirk Academy Positive Behaviour Policy;
3.7.4. Leodis Academies Trust Safe Working Practice (for staff);
3.7.5. Guidance for staff working in educational settings on the use of digital technologies and social media (staff); and
3.7.6. Leodis Academies Trust Data Protection Policy.

4. IMPLEMENTATION OF THE POLICY

4.1. The SLT will ensure all members of school staff are aware of the contents of this policy and the use of any new technology within school.

4.2. All staff, students, occasional and external users of our school ICT equipment will sign the relevant AUP.

4.3. All amendments will be published and awareness sessions will be held for all members of the school community.

4.4. Online Safety will be taught as part of the curriculum in an age-appropriate way to all students.

4.5. Online Safety posters and advice will be prominently displayed around the school.

4.6. The Online Safety Policy will be made available to parents and others via the school website.

5. RESPONSIBILITIES OF THE SCHOOL COMMUNITY

5.1. We believe that Online Safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

5.2. The Principal is responsible for:

5.2.1. Ensuring that Online Safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teaching training and safeguarding.
5.2.2. Supporting the DSL and Deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to Online Safety.
5.2.3. Ensuring staff receive regular, up-to-date and appropriate Online Safety training and information as part of their induction and safeguarding training.
5.2.4. Ensure that all staff, students and other users agree to the AUP and that new staff have Online Safety included as part of their induction.
5.2.5. Ensuring Online Safety practices are audited and evaluated.
5.2.6. Supporting staff to ensure that Online Safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of Online Safety.
5.2.7. Organising engagement with parents to keep them up to date with current Online Safety issues and how the school is keeping students safe.
5.2.8. Working with the DSL and Governing Board to update this policy on an annual basis.

5.3. Online Safety Lead

The DSL is responsible for:

5.3.1. Taking the lead for Online Safety in the school.
5.3.2. Acting as the named point of contact in school on all online safeguarding issues.
5.3.3. Undertaking training so they understand the risks associated with Online Safety and can recognise additional risks that students with SEND face online.
5.3.4. Liaising with relevant staff on Online Safety matters, for example the SENDCo and ICT Technicians.
5.3.5. Ensuring Online Safety is recognised as part of the school's safeguarding responsibilities and that a co-ordinated approach is implemented.
5.3.6. Ensuring safeguarding is considered in the school's approach to remote learning.
5.3.7. Ensuring appropriate referrals are made to external agencies, as required.
5.3.8. Keeping up-to-date with current research, legislation and online trends.
5.3.9. Co-ordinating the school's participation in local and national online safety events, for example Safer Internet Day.

5.3.10. Establishing a procedure for reporting Online Safety incidents and inappropriate internet use, both by students and staff.
5.3.11. Ensuring all members of the school community understand the reporting procedure.
5.3.12. Maintaining records of reported Online Safety concerns as well as the actions taken in response to concerns.
5.3.13. Monitoring Online Safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
5.3.14. Working with the Principal and Governing Board to update this policy on an annual basis.

5.4. Staff

5.4.1. **Read, understand and help** promote the school's Online Safety policy and guidance.
5.4.2. **Read, understand and adhere to** the staff AUP.
5.4.3. Take responsibility for ensuring the safety of sensitive school data and information.
5.4.4. Develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work.
5.4.5. Maintain a professional level of conduct in their personal use of technology at all times.
5.4.6. Ensure that all digital communication with students is on a professional level and only through school based systems, NEVER through personal email, text, mobile phone social network or other online medium.
5.4.7. Embed Online Safety messages in learning activities where appropriate.
5.4.8. Supervise students carefully when engaged in learning activities involving technology.
5.4.9. Ensure that students are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable.
Be familiar with, and understand, the indicators that students may be unsafe online.
5.4.10. Report all Online Safety incidents which occur in the appropriate log and/or to their line manager and/or the Online Safety Lead.
5.4.11. Respect and share with students the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
5.4.12. Additional responsibilities of technical staff
5.4.12.1. Support the school in providing a safe technical infrastructure to support learning and teaching.
5.4.12.2. Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date.
5.4.12.3. Ensure that provision exists for misuse detection and malicious attack.
5.4.12.4. At the request of the Leadership team, conduct occasional checks on files, folders, email and other digital content to ensure that the AUP is being followed.
5.4.12.5. Report any Online Safety related issues that come to their attention to the Online Safety lead and/or SLT.
5.4.12.6. Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management.
5.4.12.7. Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment.
5.4.12.8. Liaise with the Local Authority and others on Online Safety issues.
5.4.12.9. Document all technical procedures and review them for accuracy at appropriate intervals.
5.4.12.10. Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

5.5. Students

5.5.1. **Read, understand and adhere to** the student AUP and follow all safe practice guidance.

5.5.2. Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school.

5.5.3. Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

5.5.4. Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening.

5.5.5. Seeking help from school staff if they are concerned about something they or a peer have experienced online.

5.5.6. Discuss Online Safety issues with family and friends in an open and honest way.

5.5.7. To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices.

5.5.8. To know, understand and follow school policies regarding Cyberbullying.

5.5.9. To agree to and sign the Home/Academy Agreement containing a statement regarding their personal use of social networks in relation to the school:
Not posting images or video footage of either Academy staff, students, images of Woodkirk Academy or Woodkirk Academy's name on any internet or social media site without prior written consent from the Principal or the Vice Principal/Behaviour & Safety

5.6. Parents

5.6.1. Help and support the school in promoting Online Safety.

5.6.2. Read, understand and promote the student AUP with their children.

5.6.3. Discuss Online Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.

5.6.4. Consult with the school if they have any concerns about their child's use of technology.

5.6.5. To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images of students.

5.6.6. To agree to and sign the home-school agreement containing a statement regarding their personal use of social networks in relation to the school:
We will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

5.7. Governing Board

5.7.1. Read, understand, contribute to and help promote Woodkirk Academy's Online Safety Policy and guidance as part of the school's overarching Safeguarding procedures.

5.7.2. Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in Online Safety awareness.

5.7.3. To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data.

5.7.4. Ensure appropriate funding and resources are available for the school to implement their Online Safety strategy.

5.8. Designated Safeguarding Staff

5.8.1. Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.

5.8.2. Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, Youth Produced Sexualised Imagery (sexting), cyberbullying and others.

5.8.3. Raise awareness of the particular issues which may arise for vulnerable students in the school's approach to Online Safety ensuring that staff know the correct child protection procedures to follow.

5.9. External users of the school systems

5.9.1. Take responsibility for liaising with the school on appropriate use of the school's IT equipment and internet, including providing an appropriate level of supervision where required.

5.9.2. Ensure that agreed AUPs are followed.

6. LEARNING AND TEACHING

6.1. We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our students' lives, not just in school but outside as well, and we believe we have a duty to help prepare our students to benefit safely from the opportunities that these present.

6.2. We will deliver a planned and progressive scheme of work to teach Online Safety knowledge and understanding and to ensure that students have a growing understanding of how to manage the risks involved in online activity. We believe that learning about Online Safety should be embedded across the curriculum and also taught in specific lessons such as in ICT and PSHRE as well as tutor periods and assemblies. This includes activities which coincide with Safer Internet Day each year. This programme is co-ordinated by the subject leads for ICG and PSHRE alongside the Designated Safeguarding Lead.

6.3. We will teach students how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and students will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

6.4. We will discuss, remind or raise relevant Online Safety messages with students routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

6.5. We will remind students about the responsibilities to which they have agreed through the AUP.

6.6. Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

7. HOW PARENTS WILL BE INVOLVED

7.1. We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

7.2. To achieve this we will offer opportunities for finding out more information through an Online Safety Information Evening, the school website and regular updates via the weekly school e-newsletter. Parents will be regularly reminded of how support can be accessed in light of any Online Safety issue, whether school related or not.

7.3. We will ask all parents to discuss the student's AUP with their child and return a signed copy to the school. We also ask parents to sign the Home school agreement which includes a statement about their use of social networks in situations where it could reflect on our school's reputation and on individuals within the school community.

7.4. We request our parents to support us in applying the Online Safety Policy.

8. MANAGING AND SAFEGUARDING IT SYSTEMS

8.1. The school will ensure that access to the school IT system is as safe and secure as reasonably possible.

8.2. Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

8.3. All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff, for example the Principal and a member of technical support.

8.4. The wireless network is protected by a secure log on which prevents unauthorised access. New users can only be given access by named individuals, for example a member of technical support.

8.5. We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

8.6. Filtering Internet access

8.6.1. Web filtering of internet content is provided by Netsweeper filtering, FortiGate firewall and eSafe systems. These systems are regularly reviewed and subject to change. This ensures that all reasonable precautions are taken to prevent access to illegal content. However it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in students in monitoring their own internet activity.

8.6.2. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

8.6.3. **Teachers are encouraged to review websites** they wish to use prior to lessons for the suitability of content. If in doubt, speak to a member of the Senior Leadership Team.

8.6.4. Notices are posted in classrooms and around school as a reminder of how to seek help.

8.7. Access to school systems

8.7.1. Woodkirk Academy decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

8.7.2. All users are provided with a log in appropriate to their key stage or role in school. Students are taught about safe practice in the use of their log in and passwords.

8.7.3. Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

8.7.4. Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

8.7.5. Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users.

8.8. Passwords

8.8.1. We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).

8.8.2. We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.

8.8.3. All students have a unique, individually-named user account and password for access to IT equipment and information systems available within school.

8.8.4. All staff and students have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.

8.8.5. The school maintains a log of all accesses by users and of their activities while using the system in order to track any Online Safety incidents.

9. USING THE INTERNET

9.1. We provide the internet to:

9.1.1. support curriculum development in all subjects;
9.1.2. support the professional work of staff as an essential professional tool;
9.1.3. enhance the school's management information and business administration systems; and
9.1.4. enable electronic communication and the exchange of curriculum and administration data with the local authority, the examination boards and others.

9.2. Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

9.3. School devices are the responsibility of the member of staff they are assigned to and when used away from school, must be password protected. It is advised that any school device is for the use of staff of Woodkirk Academy only as any content, either online or offline, **is their responsibility** and any unacceptable use may result in disciplinary action. All school ICT equipment is monitored.

9.4. All users of the school IT or electronic equipment will abide by the relevant AUP at all times, whether working in a supervised activity or working independently.

9.5. Students and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school. If in classrooms, students should report directly to the class teacher. Outside the classroom, this should reported to the relevant Year Tutor or a member of the pastoral team.

9.6. Where possible, staff should refrain from using personal 3G/4G/5G data plans whilst on the school premises. In the event that staff must access the internet and the school system is down, they should act professionally at all times and be mindful of the Keeping Children Safe in Education documentation.

10. ICT MONITORING

10.1. All school devices used by staff and students are monitored using software provided by an external company. Any inappropriate use of machines, whether online or offline, will be reported to the Online Safety lead and follow up action taken if and when it is necessary. The software also monitors the use of school machines when taken off site.

10.2. Extremism and Radicalisation

10.2.1. On 1 July 2015 the Prevent Duty (section 26) of The Counter-Terrorism and Security Act 2015 came into force. This duty places the responsibility on local authorities and schools to have due regard for the need to prevent people from being drawn into terrorism.

10.2.2. Woodkirk Academy is fully committed to safeguarding and promoting the welfare of all its students. As a school we recognise that safeguarding against radicalisation is as important as safeguarding against any other vulnerability.

10.2.3. We recognise the threat that students can be exposed to online and educate students in relation to this. Parents are provided with information and resources to support this.

10.2.4. All staff are expected to uphold and promote the fundamental principles of British values, including democracy, the rule of law, individual liberty, mutual respect, and tolerance of those with different faiths and beliefs. We believe that children should be given the opportunity to explore diversity and understand Britain as a multi-cultural society; everyone should be treated with respect whatever their race, gender, sexuality, religious belief, special need, or disability. As part of our commitment to safeguarding and child protection we fully support the Government's Prevent Strategy

10.2.5. With effect from 1 July 2015, the Counter-Terrorism and Security Act 2015 introduced the Prevent Duty and schools, colleges and other specified authorities, including local authorities, health and the police ‘to have due regard to the need to prevent people from being drawn into terrorism.’

10.2.6. The Academy uses software to monitor all computer activity, both online and offline, with appropriate filtering to ensure all students and staff are protected against exposure to violent extremist material. Any inappropriate activity is referred directly to the Designated Safeguarding Lead and appropriate action taken.

10.2.7. If staff are concerned about a change in the behavior of an individual or see something that concerns them (this could be a colleague too) they must seek advice appropriately with the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead who must contact the Education Safeguarding Team or the Prevent Education Officer– Julia Holden, 07891 273720 for further information contained with the Safeguarding & Child Protection Policy.

10.3. Cyberbullying

10.3.1. Cyberbullying can include the following:

10.3.1.1. Threatening, intimidating or upsetting text messages.
10.3.1.2. Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
10.3.1.3. Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
10.3.1.4. Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.
10.3.1.5. Menacing or upsetting responses to someone in a chatroom.
10.3.1.6. Unpleasant messages sent via instant messaging.
10.3.1.7. Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, for example Facebook.

10.3.2. Cyberbullying against students or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy and Positive Behaviour Policy.

10.3.3. Peer-on-peer sexual abuse and harassment

10.3.3.1. Students may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that students are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

10.3.3.2. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

10.3.3.2.1. Threatening, facilitating or encouraging sexual violence.
10.3.3.2.2. Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.
10.3.3.2.3. Sexualised online bullying, for example sexual jokes or taunts.
10.3.3.2.4. Unwanted and unsolicited sexual comments and messages.
10.3.3.2.5. Consensual or non-consensual sharing of sexualised imagery.

10.3.3.3. Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

10.3.3.4. The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL or another member of the Designated Safeguarding Team, who will investigate the matter in line with the Positive Behaviour Policy and the Safeguarding and Child Protection Policy.

10.3.3.5. Sharing of nudes and semi-nudes:

Any reported instances involving the sharing of nudes and semi-nudes will be dealt with by the Designated Safeguarding Team. This may include support from the Safer Schools Officer. Parents will always be notified. The sharing of sexualised imagery of individuals under the age of 18 is illegal regardless of whether consent was given by the subject of the imagery. Where there are reports or concerns around non-consensual sharing of images, school will always liaise with the Safer Schools Officer due to the fact that this may be abusive behaviour. This may also result in further disciplinary action by school.

All students are educated in school around the risks and potential consequences of sharing sexualised imagery. Further individualised support will be offered to students as necessary, particularly those with increased vulnerabilities.

10.3.4. Grooming and exploitation

10.3.4.1. Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

10.3.4.2. Staff will be aware that grooming often takes place online and that students who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

10.3.4.2.1. The student believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.

10.3.4.2.2. The student does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.

10.3.4.2.3. The student may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.

10.3.4.2.4. Talking to someone secretly over the internet may make the student feel 'special', particularly if the person they are talking to is older.

10.3.4.2.5. The student may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

10.3.4.3. Due to the fact students are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

10.3.4.3.1. Being secretive about how they are spending their time.
10.3.4.3.2. Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
10.3.4.3.3. Having money or new possessions, for example clothes and technological devices, that they cannot or will not explain.

10.3.5. Child sexual exploitation (CSE) and child criminal exploitation (CCE)

10.3.5.1. Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, for example sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a student may be groomed online to become involved in a wider network of exploitation, for example the production of child pornography or forced child prostitution and sexual trafficking.

10.3.5.2. CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, for example drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

10.3.5.3. Where staff have any concerns about students with relation to CSE or CCE, they will bring these concerns to the DSL/Designated Team without delay, who will manage the situation in line with the Safeguarding and Child Protection Policy.

10.3.6. Mental health

10.3.6.1. The internet, particularly social media, can be the root cause of a number of mental health issues in students, for example low self-esteem and suicidal ideation.

10.3.6.2. Staff will be aware that online activity both in and outside of school can have a substantial impact on student's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a student is suffering from challenges in their mental health.

10.3.7. Online hoaxes and harmful online challenges

10.3.7.1. For the purposes of this policy, an **'online hoax'** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

10.3.7.2. For the purposes of this policy, **'harmful online challenges'** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

10.3.7.3. Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the school, they will report this to the DSL immediately.

10.3.7.4. The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the Local Authority about whether quick local action can prevent the hoax or challenge from spreading more widely.

10.3.7.5. Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Principal will decide whether each proposed response is:

10.3.7.5.1. In line with any advice received from a known, reliable source, for example the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
10.3.7.5.2. Careful to avoid needlessly scaring or distressing students.

10.3.7.5.3. Not inadvertently encouraging students to view the hoax or challenge where they would not have otherwise come across it, for example where content is explained to younger students but is almost exclusively being shared amongst older students.
10.3.7.5.4. Proportional to the actual or perceived risk.
10.3.7.5.5. Helpful to the students who are, or are perceived to be, at risk.
10.3.7.5.6. Appropriate for the relevant students' age and developmental stage.
10.3.7.5.7. Supportive.
10.3.7.5.8. In line with the Safeguarding and Child Protection Policy.

10.3.7.6. Where the DSL's assessment finds an online challenge to be putting students at risk of harm, for example it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, for example those within a particular age range that is directly affected or even to individual children at risk where appropriate.

10.3.7.7. The DSL and Principal will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing students' exposure to the risk is considered and mitigated as far as possible.

10.3.8. Cyber-crime

10.3.8.1. Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

10.3.8.1.1. **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, for example fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

10.3.8.1.2. **Cyber-dependent** – these crimes can only be carried out online or by using a computer, for example making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

10.3.8.2. The school will factor into its approach to Online Safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to further support via routes such as the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

10.3.8.3. The DSL and Principal will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, for example the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

11. USING EMAIL

11.1. Email is regarded as an essential means of communication and Woodkirk Academy provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, students and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of Woodkirk Academy is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

11.2. Use of the school e-mail system is monitored and checked.

11.3. It is the personal responsibility of the email account holder to keep their password secure.

11.4. As part of the curriculum students are taught about safe and appropriate use of email. Students are informed that misuse of email may result in a loss of privileges.

11.5. Woodkirk Academy will set clear guidelines detailing when student-staff communication via email is acceptable and staff may set clear boundaries for students on the out-of-school times when emails may be answered.

11.6. Under no circumstances will staff contact students or parents, or conduct any school business using a personal email address.

11.7. Responsible use of personal web mail accounts on school systems is permitted outside teaching hours.

12. SOCIAL NETWORKS

12.1. If any student attempts to make contact with a member of staff via social networks, this must be referred to Mr D Currie or another member of the Senior Leadership Team.

12.2. It is accepted that a number of staff may have their own social network accounts. Such accounts should not, under any circumstances, be used to communicate with students.

12.3. It is strongly recommended that security/privacy settings should be set to ensure all content is private and not freely available for students or parents to access.

12.4. Staff are strongly advised against contact with ex-students via social networks, such as having them as 'friends' or contacts via Facebook and Twitter.

12.5. Staff are strongly advised against linking themselves to Woodkirk Academy on social networks, for example naming it as a place of work on Facebook.

12.6. While access to social media sites through the Academy network is blocked to employees, accessing the internet through mobile phones and other mobile devices is prohibited during working hours. Staff should never use Academy networks or equipment to access or update a social media site.

12.7. Staff must be aware of how to set privacy settings on their profile and be mindful that some social networking sites revert to default settings when an update is made to their service. Staff should be vigilant to any changes in their profile privacy settings.

12.8. Further guidance and advice is provided for staff in the Use of Digital Technologies and Social Media Code of Practice

13. PUBLISHING CONTENT ONLINE

13.1. Publishing content online includes using the Woodkirk Academy website, Learning Platform, blogs, wikis, podcasts, social network sites and personal web pages.

13.2. Woodkirk Academy website

13.2.1. Woodkirk Academy maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The Academy maintains the integrity of its website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

13.2.2. Identities of students are protected at all times. Photographs of identifiable individual students are not published on the website and school obtains permission from parents for the use of students' photographs. Group photographs do not have a name list attached.

13.3. Creating online content as part of the curriculum

13.3.1. As part of the curriculum we encourage students to create online content. Students are taught safe and responsible behavior in the creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Personal publishing of online content is taught via age-appropriate sites that are suitable for educational purposes. They are moderated by the school where possible. Students will only be allowed to post or create content on sites where members of the public have access when this is part of a school related activity. Appropriate procedures to protect the identity of students will be followed.

13.3.2. We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

13.4. Online material published outside the school

13.4.1. Staff and students are encouraged to adopt safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

13.4.2. Material published by students, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of, another student or member of the school community will be considered a serious breach of school discipline and treated accordingly.

14. USING IMAGES, VIDEO AND SOUND

14.1. We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Students are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

14.2. Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of students wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

14.3. We ask all parents to sign an agreement about taking and publishing photographs and video of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

14.4. We secure additional parental consent specifically for the publication of students' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly on the website.

14.5. For their own protection, staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of students.

14.6. We are happy for parents to take photographs at school events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites.

15. USING VIDEO CONFERENCING, WEB CAMERAS AND OTHER ONLINE MEETINGS

15.1. We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow students to link up with people in other locations and see and hear each other. We ensure that staff and students take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Students do not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

15.2. Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

15.3. All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

15.4. For their own protection a video conference or other online meeting between a member of staff and student(s) which takes place outside school or whilst the member of staff is alone is always conducted with the prior knowledge of the head teacher or line manager and respective parents.

16. USING MOBILE PHONES

16.1. Use of mobile phones by students is covered by a separate policy and they are not permitted on site during the school day under any circumstances.

16.2. During lesson time we expect all mobile phones belonging to staff to be switched off or on silent unless there is a specific agreement for this not to be the case.

16.3. Where required for safety reasons in off-site activities, a school mobile phone is provided for staff for contact with students, parents or the school. **Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.**
In an emergency, where a staff member does not have access to a school-owned device or given direct permission by a member of the Senior Leadership Team they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

16.4. Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another student or staff member we do not consider it a defense that the activity took place outside school hours.

16.5. The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter. Further information on 'cyberbullying' can be found in the Anti-Bullying Policy.

16.6. We make it clear to staff, students and parents that the Principal has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred. Please refer to 8.6, which relates to the use of 3G/4G/5G.

17. USING OTHER TECHNOLOGIES

17.1. We will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an Online Safety point of view.

17.2. We will regularly review the Online Safety Policy to reflect any new technology that we use, or to reflect the use of new technology by students.

17.3. Staff or students using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

18. PROTECTING SCHOOL DATA AND INFORMATION

18.1. Woodkirk Academy recognises its obligation to safeguard sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

18.2. The Academy is a registered Data Controller under GDPR and the Data Protection Act 2018 and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.

18.3. Students are taught about the need to protect their own personal data as part of their Online Safety awareness and the risks resulting from giving this away to third parties.

18.4. Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

18.4.1. All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended.

18.4.2. Staff are provided with appropriate levels of access to the school management information system holding student data. Passwords are not shared and administrator passwords are kept secure.

18.4.3. Staff are aware of their obligation to keep sensitive data secure when working on computers outside school.

18.4.4. All devices taken off site, for example laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.

18.4.5. When we dispose of old computers and other equipment our recycler ensures that the data is destroyed and certifies that this has been done.

18.4.6. We follow clear procedures for transmitting data securely and sensitive data is not sent via email unless encrypted.

18.4.7. Remote access to computers is by authorised personnel only.

18.4.8. We have full back up and recovery procedures in place for school data.

18.4.9. Where sensitive staff or student data is shared with other people who have a right to see the information, for example Governors or School improvement officers, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies.

19. MANAGEMENT OF ASSETS

19.1. Details of all school-owned hardware and software are recorded in an inventory.

19.2. All redundant IT equipment is 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.

19.3. Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

20. MANAGING ONLINE SAFETY

20.1. All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

20.2. The DSL has overall responsibility for the school's approach to Online Safety, with support from other members of the Senior Leadership Team, Designated Safeguarding Team and the Principal where appropriate, and will ensure there are strong processes in place to handle any concerns about students' safety online.

20.3. The importance of Online Safety is integrated across all school operations in the following way:

20.3.1. Staff receive regular training, at least once each academic year.

20.3.2. Staff receive regular email updates regarding Online Safety information and any changes to Online Safety guidance or legislation.

20.3.3. Online Safety is integrated into learning throughout the curriculum.

20.3.4.

20.3.5. Assemblies and Form Time activities are used to educate students about keeping themselves safe online.

21. DEALING WITH ONLINE SAFETY INCIDENTS

21.1. All Online Safety incidents are recorded in the School Online Safety Log on CPOMS which is regularly reviewed. All reports from Esafe are uploaded directly into CPOMS and followed up by a member of the pastoral team. Parents are alerted when necessary.

21.2. Any incidents where students do not follow the AUP will be dealt with following the school's normal behaviour or disciplinary procedures.

21.3. In situations where a member of staff is made aware of a serious Online Safety incident, concerning students or staff, they will inform the Online Safety Lead (DSL) or Deputy DSL, their line manager or Principal who will then respond in the most appropriate manner.

21.4. Instances of cyberbullying will be taken very seriously by the Academy and dealt with using our anti-bullying procedures. We recognise that staff as well as students may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim. The Safer Schools Officer is most likely to be involved in such instances. (Further information is contained within the Anti-Bullying and Harassment Policy. This includes a section with specific references to Hate Incidents

21.5. Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Online Safety Lead and technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

21.6. Woodkirk Academy reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

21.7. Dealing with a Child Protection issue arising from the use of technology

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Academy's Safeguarding Procedures and Guidance will be followed. A member of the Designated Safeguarding Team will liaise with the police and other agencies where necessary.

21.8. Dealing with complaints and breaches of conduct by students

21.8.1. Any complaints or breaches of conduct will be dealt with promptly
21.8.2. Responsibility for handling serious incidents will be given to a senior member of staff
21.8.3. Parents and the student will work in partnership with staff to resolve any issues arising
21.8.4. Restorative practice will be used to support the victims
21.8.5. There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.
21.8.6. Further intervention will be put in place for individuals when necessary. This may be, for example 1 to 1 support from the Safer Schools Officer or a Learning Mentor. In some instances, support may be required from other agencies, such as CEOP.
21.8.7. The school avoids unnecessarily criminalising students, for example calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, for example a student has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

21.9. The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal). The following apply to all members of the school community

21.9.1. Accessing inappropriate or illegal content deliberately.
21.9.2. Deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
21.9.3. Continuing to send or post material regarded as harassment, or of a bullying nature after being warned.
21.9.4. Staff using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites).
21.9.5. Involvement with instances of Youth Produced Sexualised Imagery (sexting).

21.10. The following activities are likely to result in disciplinary action

21.10.1. Any online activity by a member of the school community which is likely to adversely impact on the reputation of the school.
21.10.2. Accessing inappropriate or illegal content accidentally and failing to report this.
21.10.3. Inappropriate use of personal technologies, for example mobile phones, at school or in lessons.

21.10.4. Sharing files which are not legitimately obtained, for example music files from a file sharing site.
21.10.5. Using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute.
21.10.6. Attempting to circumvent school filtering, monitoring or other security systems.
21.10.7. Circulation of commercial, advertising or 'chain' emails or messages.
21.10.8. Revealing the personal information (including digital images, videos and text) of others by electronic means, for example sending of messages, creating online content without permission.
21.10.9. Using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content).
21.10.10. Transferring sensitive data insecurely or infringing the conditions of GDPR and the Data Protection Act 2018.

21.11. The following activities would normally be unacceptable; in some circumstances they may be allowed, for example as part of planned curriculum activity or by a system administrator to problem solve (permission would be from the Online Safety Lead)

21.11.1. Accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time.
21.11.2. Accessing non-educational websites (for example gaming or shopping websites) during lesson time.
21.11.3. Sharing a username and password with others or allowing another person to log in using your account.
21.11.4. Accessing school ICT systems with someone else's username and password.
21.11.5. Deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else.