



Woodside Group Online Safety Policy

Online Safety Policy

Policy Owner: Head of Compliance
Date of Issue: July 2022
Last scheduled review: Aut 24
Next scheduled review: Aut 25



Woodside Group Online Safety Policy

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	4
4. Educating pupils about online safety	7
5. Educating parents about online safety	9
6. Cyber-bullying	9
7. Acceptable use of the internet in school	11
8. Pupils using mobile devices in school	11
9. Staff using work devices outside school	12
10. How the school will respond to issues of misuse	12
11. Training	13
12. Monitoring arrangements	14
13. Links with other policies	14
Appendix 1: Acceptable use agreement (primary pupils)	15
Appendix 2: Acceptable use agreement (secondary pupils)	17
Appendix 3: Acceptable use agreement (staff & volunteers)	19
Appendix 4: Online safety training needs – self audit for staff	24
Appendix 5: Online safety incident report log	25



Woodside Group Online Safety Policy

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, and where applicable, volunteers and visitors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)

Policy Owner: Head of Compliance
Date of Issue: July 2022
Last scheduled review: Aut 24
Next scheduled review: Aut 25



Woodside Group Online Safety Policy

- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

Organisational Lead: Jonathan Lakin (CEO & Proprietor of the Woodside Group)

3.1 Directors of the Woodside Group and Executive Headteacher

The Directors of the Woodside Group have overall responsibility for monitoring this policy and holding the school headteacher(s) to account for its implementation. They will be assisted in this duty by the Executive Headteacher.

The Directors of the Woodside Group will ensure the co-ordination of regular meetings with appropriate staff/managers to discuss online safety, and will, alongside the Head of Compliance, monitor online safety logs as provided by the school designated safeguarding lead (DSL).

The Director who oversees online safety is the Director of Education.

3.2 The Head of Compliance

The Head of Compliance is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. This role will also ensure that Headteachers/DSLs maintain accurate records of online safety incidents, and that appropriate actions are taken when they arise.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL/Headteacher takes lead responsibility for online safety in school, in particular:

Policy Owner: Head of Compliance
Date of Issue: July 2022
Last scheduled review: Aut 24
Next scheduled review: Aut 25



Woodside Group Online Safety Policy

- Ensuring that staff in their school understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of Compliance, IT technician and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school Safeguarding & Child Protection policy
- Ensuring that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating staff training on online safety, and ensuring that all student-facing staff receive this training (Appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of Compliance/Director of Education

3.4 The IT technician/Contractor

The IT technician/contractor is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a half-termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy



Woodside Group Online Safety Policy

3.5 All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3), and ensuring that pupils follow the school's terms on acceptable use (Appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)



Woodside Group Online Safety Policy

3.7 Visitors, contractors and members of the community

Visitors, contractors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3). **All visitors and contractors are required to read the 'Visitor Safeguarding & Safety Notice', which details key expectations regarding online use in school.**

4. Educating pupils about online safety

Pupils will be taught about online safety primarily through the school's PSHE curriculum (which incorporates 'Relationships Education' at primary level, and 'Relationships and Sex Education' at secondary level).

Pupils in the primary school phase will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of the primary school phase, pupils should know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)



Woodside Group Online Safety Policy

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Pupils in the secondary school phase will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of the secondary school phase, pupils should know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours



Woodside Group Online Safety Policy

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant (eg; Personal Progress, Skillsbuilder lessons)

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via the school website.

Aspects of online safety will also be covered during parent visits.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Headteacher/Head of Base.

Concerns or queries about this policy can be raised with any member of staff or the relevant Headteacher/Head of Base.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.



Woodside Group Online Safety Policy

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Safeguarding & Child Protection Policy, Student Behaviour Policy and the Equality, Diversity and Inclusion Policy (if applicable). Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*



Woodside Group Online Safety Policy

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, and where applicable, volunteers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors and contractors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

The school does **not** permit students to bring mobile phones into school buildings, and they are on the list of 'items banned under the school rules' (as explained in the current school Behaviour Policy).

In the event that a student brings in a mobile phone with them to school, prior to entering the school base/main building, they **MUST**:

- Submit mobile phones to Headteachers/Heads of Base/other nominated school staff. These will be securely locked away and handed back to students at the car park before they leave for home

****Exceptions (all exceptions will be risk-assessed, and a student 'behavioural contract' set up prior to agreement/use):***



Woodside Group Online Safety Policy

- Portable gaming devices such as a Nintendo DS may be made available to students at certain times at the discretion of the Headteacher/Head of Base, if it is known to significantly aid students in their ability to self-regulate at times of stress/anxiety
- At the discretion of the Headteacher/Head of Base, students may bring in a portable device (including old mobile phones with no SIM card) used for listening to music during the school day, as a tool to aid with self-regulation/ reduce anxiety

Any agreed use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendices 1 and 2).

9. Staff using work devices inside and outside school

All staff members will take appropriate steps to ensure their devices remain secure (appropriate support will be provided by the IT Technician). This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring that the password used to access the school's IT systems are changed regularly (at least every 6 months)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Technician.

10. How the school will respond to issues of misuse

Policy Owner: Head of Compliance
Date of Issue: July 2022
Last scheduled review: Aut 24
Next scheduled review: Aut 25



Woodside Group Online Safety Policy

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures as set out in the school Safeguarding & Child Protection policy, Student Behaviour Policy, and the Student Acceptable Use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff Disciplinary Policy and procedures/staff code of conduct (GSWP 2022). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive safeguarding and child protection training (to include online safety), which is regularly updated (for example through weekly 'Safeguarding Snippets', emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:



Woodside Group Online Safety Policy

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL (and deputies) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

Monitoring of online activity in school takes place on a regular basis, and is overseen by the DSL and IT Lead, who will review reports and activity via the Barracuda filtering & monitoring system. The monitoring system picks up incidents promptly, and will send alerts to the DSL and IT Lead, so that a prompt investigation and response can be undertaken.

Additional monitoring systems used by the school include:

- Staff physically monitoring by watching users' screens; staff must, at all times, ensure that they have full visibility of the screen, when students are working on a laptop/computer/tablets

The school's filtering and monitoring provision is reviewed annually.

The DSL/DDSLs log behaviour and safeguarding issues related to online safety. An example incident report log can be found in appendix 5.

This policy will be reviewed annually by the Head of Compliance and IT Lead.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy

Policy Owner: Head of Compliance
Date of Issue: July 2022
Last scheduled review: Aut 24
Next scheduled review: Aut 25



Woodside Group Online Safety Policy

- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy



Woodside Group Online Safety Policy

APPENDIX 1

Acceptable Use of Internet Policy (for Primary Pupils)



ZIP IT

Keep your personal stuff private and think about what you say and do online.



BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.



FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

To keep me safe whenever I use the internet or email, I promise...



- to keep my usernames and passwords private and not to use anyone else's
- to keep all personal information private



- to block unknown links and attachments by not opening anything that I do not trust



- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer equipment in school...

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own

Policy Owner: Head of Compliance

Date of Issue: July 2022

Last scheduled review: Aut 24

Next scheduled review: Aut 25



Woodside Group Online Safety Policy

- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

If I break these rules...

- I understand that the school's behaviour guidelines will be followed, and I may not be able to use the internet for a period of time

I have read and understand this policy and agree to follow it.

Name of pupil _____

Signed _____ Date _____



Woodside Group Online Safety Policy

APPENDIX 2

Acceptable Use of Internet Policy (for Secondary Pupils)



ZIP IT

Keep your personal stuff private and think about what you say and do online.



BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.



FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.



- I will not share any of my usernames and passwords or try to use anyone else's
- I will not post online any personal information about myself or others



- I will block attachments to emails by not opening anything sent that I do not trust or recognise – it may contain a virus



- I will immediately report any messages or internet content that is inappropriate or makes me feel uncomfortable
- I will immediately report any damage or faults involving equipment or software

- I understand that the school will monitor my use of school computer equipment and the internet
- I will not use the school ICT systems for personal or recreational use unless I have permission to do so
- I will respect other people's work and property and will not access, copy, remove or otherwise alter anyone else's files, without their permission
- I will be polite and responsible when I communicate with others online, including when undertaking remote learning
- I will not take or distribute images of anyone at school

Policy Owner: Head of Compliance
Date of Issue: July 2022
Last scheduled review: Aut 24
Next scheduled review: Aut 25



Woodside Group Online Safety Policy

- I will only use my mobile phone and other handheld devices in accordance with the school policy
- I will not try to upload, download or access any materials which are illegal or inappropriate
- I will not use any way of trying to bypass the filtering / security systems, designed to prevent access to inappropriate material
- I will not try to install any programmes on a school computer nor alter the settings
- I will only use chat and social networking sites with permission and at the times that are allowed, in accordance with the school policy
- I will respect the copyright of others in my own work
- I will not try to download pirate copies of music, videos, games or other software
- I will take care to check that information I use is accurate
- I understand that if I break this agreement, the school will take action according to the school behaviour guidelines
- I understand that Police could be involved if something I did was illegal

I have read and understand this policy and agree to follow it.

Name of student _____

Signed _____ Date _____



Woodside Group Online Safety Policy

APPENDIX 3

Acceptable Use of Internet Policy (for Staff & Volunteers)



ZIP IT

Keep your personal stuff private and think about what you say and do online.



BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.



FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.



- I will not share any of my usernames and passwords or try to use anyone else's
- I will not post online any personal information about myself or others



- I will block attachments to emails by not opening anything sent that I do not trust or recognise – it may contain a virus



- I will immediately report any messages or internet content that is inappropriate or makes me feel uncomfortable
- I will immediately report any damage or faults involving equipment or software

School Policy

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

This Acceptable Use policy is intended to ensure:

Policy Owner: Head of Compliance
Date of Issue: July 2022
Last scheduled review: Aut 24
Next scheduled review: Aut 25



Woodside Group Online Safety Policy

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the school utilises a filtering system to block inappropriate/ harmful content
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are Intended for educational use only.



Woodside Group Online Safety Policy

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the 'Bring your own device' policy.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult



Woodside Group Online Safety Policy

pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer without permission.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:



Woodside Group Online Safety Policy

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.
- I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

I have read and understand this policy and agree to follow it.

Full name: _____

Signed: _____ Date: _____



Woodside Group Online Safety Policy

APPENDIX 4: Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT (CONDUCTED VIA PORTAL FORM)	
Questions	
Do you know the name of the person who has lead responsibility for online safety in school?	Please list the names of any live-streaming apps that students/pupils at your base use, that you are aware of
Are you aware of the ways pupils can abuse their peers online?	Please list the names of any social network platforms that students/pupils at your base use, that you are aware of
Do you know what you must do if a pupil approaches you with a concern or issue?	How would you rate your awareness of the aspects of online safety being taught at your base (either through discrete subjects/lessons, or via cross-curricular/themed approaches)?
Are you familiar with the school's acceptable use agreement for staff?	How would you rate your awareness/knowledge of the school's approach to tackling cyber-bullying?
Are you familiar with the school's acceptable use agreement for pupils?	Are there any specific areas of online safety in which you would like training/further training?
Do you regularly (at least every 6 months) change your password for accessing the school's IT systems?	



Woodside Group Online Safety Policy

[APPENDIX 5: Online safety incident report log \(for DSL/DDSL use\)](#)

ONLINE SAFETY INCIDENT LOG				
Date incident took place	Where the incident took place	Description of the incident	Action taken and by whom	Name of staff member initially recording the incident on 'safeguarding portal form'

Policy Owner: Head of Compliance
 Date of Issue: July 2022
 Last scheduled review: Aut 24
 Next scheduled review: Aut 25