Woodbrook Vale School
Policy Document

Online Safety Policy

Date First Approved by the Trustees: 09 February 2023

Review Date Annually: Headteacher Approval Summer Term 2024

Headteacher’s Signature: RFraser ……………………………..…………….. Date: 09 February 2023

Print name: Rachael Fraser

Data will be processed to be in line with the requirements and protections set out in the UK General Data Protection Regulation.

Stakeholders	Formulation	Review
Trustees	N/A	Y
SLT	Y	Y
Staff working group	Y	N
Parent Forum	N	N
Students	N	N
Other …………….		

Contents

Schedule for Development/Monitoring/Review

This Online Safety Policy was approved by the Board of Trustees:

The Online Safety Policy will be reviewed annually, by the Headteacher or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The School will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Surveys/questionnaires of
  - Students
  - Parents/carers
  - Staff

Scope of the Policy

This policy applies to all members of Woodbrook Vale School (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Woodbrook Vale School ICT Systems, both in and out of Woodbrook Vale School.

The Education and Inspectors Act 2006 empowers Headteachers to such extent as is responsible, to regulate the behaviour of the students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is the pertinent to incidents of Online Bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and or electronic devices and the deletion of data.

Woodbrook Vale School will deal with such incidents within this policy and associated behaviour and anti-bullying polices will, where known, inform parents/carers of incidents and inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within Woodbrook Vale School.

Trustees

Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by trustees receiving regular information about Online Safety incidents and monitoring reports.

Headteacher

The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.

- The Headteacher and (at least) another member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- The Headteacher/Senior Leadership Team are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-Ordinator.

ICT Systems Manager

The ICT Systems Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required Online technical requirements and any Local Authority/other relevant body Online Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant.
- that the use of the network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Online Safety Coordinator for any investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in school policies.

Online Safety Coordinator

- leads the Online Safety working group (School Business Manager, ICT Systems Manager, Head of Business and Computing Faculty, DSL)
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
- reports regularly to Senior Leadership Team.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the Headteacher, Online Safety Coordinator, ICT Systems Manager
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Leads

Receive training in Online Safety issues and are aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students

are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy. Students will be taught through lessons, assemblies and the Personal Development Programme to:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand policies on the use of mobile devices and digital cameras.
- know and understand policies on the taking / use of images and on cyber-bullying.
- Know and understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local Online Safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student records
- their children's personal devices in the school

Education – Students

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

Online Safety will be a focus in all areas of the curriculum and staff will reinforce Online Safety messages across the curriculum. The Online Safety curriculum aims to be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety curriculum will be provided as part of ICT/PD/assemblies/tutor led other lessons and is revisited annually (or more frequently if new 'tech' issues arise).
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, students will be guided to sites checked recently as suitable for their use. In the event of any unsuitable material being found in internet searches, this will be reported immediately to the ICT Systems Manager who will alert the appropriate member of SLT who will conduct an investigation.
- Where students are allowed to freely search the internet, filters are in place to block access to most content that is inappropriate. Staff will be vigilant however, in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, a member of SLT staff can request the temporary removal of names sites from the filtered list for the period of study. For the purposes of transparency and audit, any request to do so, will be sent by email to the ICT Systems Manager, with clear reasons for the need.

Education – Parent/Carers

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day

Education – The Wider Community

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

Education and Training – Staff/Volunteers

All staff will receive Online Safety training as part of Safeguarding Training and as standalone sessions. These sessions aim to help staff to understand their responsibilities, as outlined in this policy. An audit of the Online Safety training needs of all staff will be carried out regularly.

Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school 'Online Safety policy' and 'Acceptable Use Agreements' and 'Safer Working Practice' document.
- The Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations, and by reviewing guidance documents released by relevant organisations. These updates will be shared with staff.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.

Training – Trustees

Trustees take part in Online Safety awareness sessions as part of their safeguarding training and as separate stand-alone sessions. Trustees who are linked to health and safety, cyber safety, ICT and safeguarding will be trained and receive updates regularly.

Training may take the form of:

- Attendance at training provided by the Local Authority/National Governors Association/Police and/or other relevant organisation.
- Participation in school training/information sessions for staff or parents

Technical – Infrastructure/Equipment, Filtering and Monitoring

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school is responsible for ensuring that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities so that:

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements.
- There are regular reviews and audits of the safety and security of school technical systems.
- All users have clearly defined access rights to school systems and devices.
- All users are provided with a username and secure password. Users are responsible for the security of their username and password.
- The school provides enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- An agreed system is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.
- Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the school's systems, without agreement from the ICT Systems Manager who will consult with his SLT link.
- Users may use the following types of removable media for the purposes detailed:
- CD/DVD – Playing of original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership) is permitted but kept to a minimum. The use of software written to writable versions of this media is strictly prohibited.
- USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited. All USB media must be encrypted for school use.
- Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

Bring Your Own Device (BYOD):

Whilst we accept that mobile technologies offer great opportunities for learning and that many students have their own devices at home, we have made sure we have suitable, equitable and widespread access to technology with a continuously open-minded approach to introducing new technologies to enhance learning. This is one reason we do not allow students to bring their own devices for learning. There are also a number of other reasons as follows:

- Use of BYOD can introduce vulnerabilities into the existing secure environment.
- Issues that require indeterminate amounts of technician time might include: faulty equipment, levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.
- Issues of inequality between ‘own’ devices would be unavoidable.

Therefore, we have taken the decision to remain a non BYOD school.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- It is school policy that images of staff and students may only be captured on a school owned device and must not be uploaded to the internet or shared. (Ipads are available)
- When using digital images staff will take the opportunity to inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others whilst on the school site.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Use of students’ full names will avoided on school websites, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website, with consent being recorded on the school’s MIS.
- Student’s work may be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the schools' GDPR and Data Protection Policy.

Staff must ensure that they:

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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers must be professional in tone and content.
- Students will be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school/ website and only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

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

The school's use of social media for professional purposes will be checked regularly.

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in. All staff receive a copy of the Online Safety Policy and a copy of the Acceptable Use Agreement, which they sign and return to the school, to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement is displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

When accessing the Learning Platform from home, the same Acceptable Use Agreement applies. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy will be followed to deal with any misconduct and all appropriate authorities contacted. Where the allegation refers to the Headteacher, the report must be made to the Chair of Trustees.

Appropriate and Inappropriate Use by Children or Young People

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

School asks parents/carers to support the agreement with their child or young person. This is shown by signing the Acceptable Use Agreements together so that it is clear to the school that the agreement is accepted by the student with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school. Further to this, it is hoped that parents/carers will adhere to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.
File-sharing via email, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

In the Event of Inappropriate Use

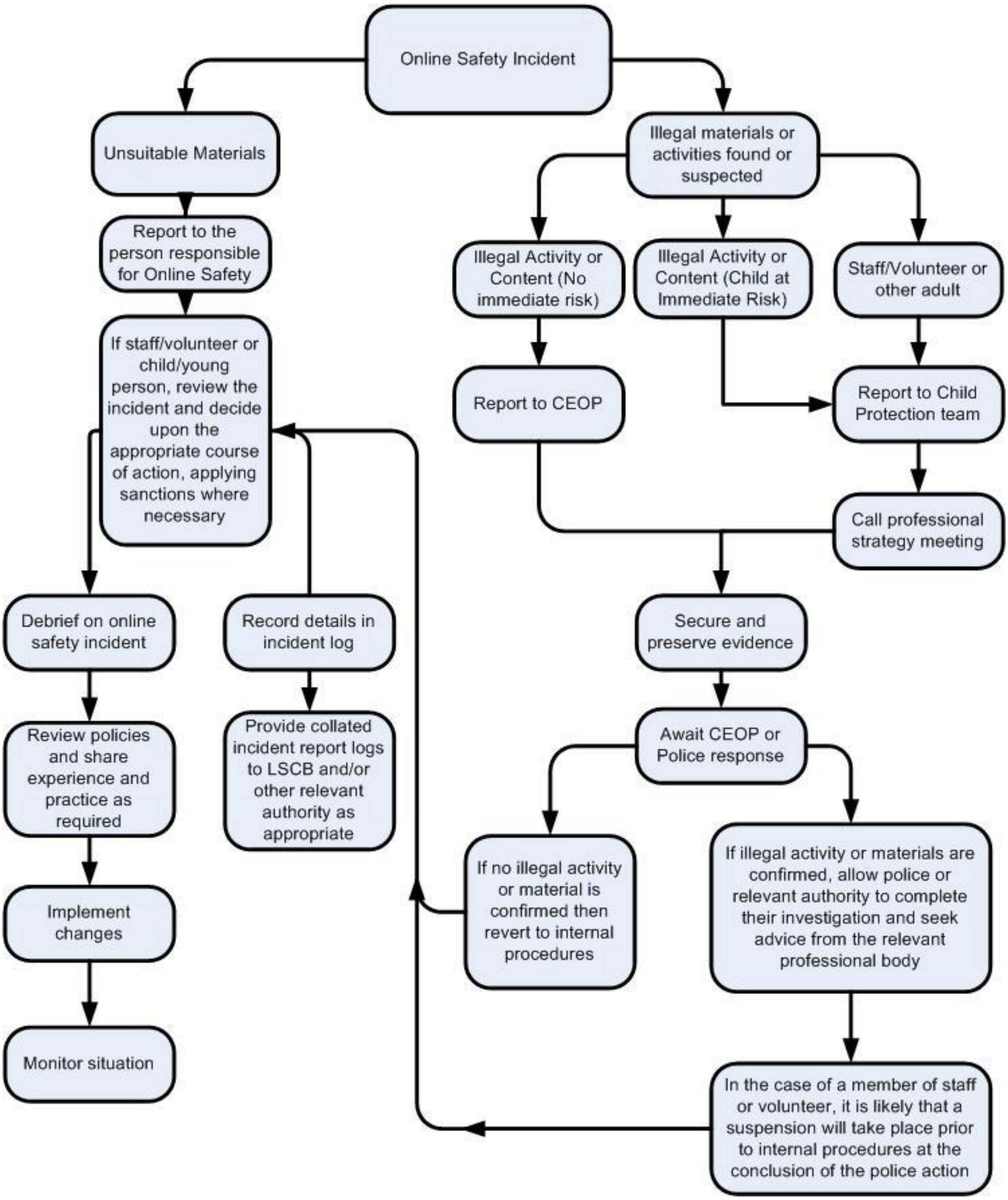
Should a child or young person be found to misuse the online facilities by not following the Acceptable Use Agreement r the Online Safety Policy, the following consequences may be used:

- Any child found to be misusing the internet may have a letter/phone call home explaining the reason for suspending the student's use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.
- A letter/phone call home may outline a breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult. In this case the school will refer to their behaviour, safeguarding and anti-bulling policies.

In the event that a child or young person accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. If a student deliberately misuses online technologies, this will be addressed by the school.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, the following procedure is in place:

- more than one senior member of staff is involved in the process to protect individuals if accusations are subsequently reported.
- Investigations will be conducted using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. (using the same computer for the duration of the investigation).
- relevant staff will have appropriate internet access to conduct an investigation, and the sites and content visited are closely monitored and recorded (to provide further protection).
- The URL of any site containing the alleged misuse is carefully retained and a description of the nature of the content causing concern is made. Screenshots of the content on the machine may need to be taken and stored for purposes of being used for investigation. (except in the case of images of child sexual abuse – see below).
- Once an incident is fully investigated the group will judge whether this concern has substance or not. If it does then appropriate action will take place and could include the following:
    1. Internal response or discipline procedures.
    2. Involvement by Local Authority or national/local organisation (as relevant).
    3. Police involvement and/or action.
    4. If content being reviewed includes images of child abuse then the monitoring will be halted and referred to the Police immediately. Other instances that will be reported to the Police are:
        - incidents of ‘grooming’ behaviour.
        - the sending of obscene materials to a child.
        - adult material which potentially breaches the Obscene Publications Act.
        - criminally racist material.
        - other criminal conduct, activity or materials.

Secure Transfer of Data and Access out of School

Woodbrook Vale School recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

Appendix 2

Aspire • Enjoy • Succeed

Woodbrook Vale School

Acceptable Use Agreement (Staff/Volunteer)

January 2022

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 internet access at all times.

This Acceptable Use Policy is intended to ensure:

- 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.
- Woodbrook Vale ICT 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 ICT in their everyday work.

Woodbrook Vale School will try to ensure that staff and volunteers will have good access to ICT 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.

This policy applies to any device in school. It applies across the whole network and includes Wi-Fi.

Woodbrook Vale School carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Woodbrook Vale School can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the internet is closely monitored by the school, logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device.

The school email system is provided for educational purposes, where required the school has the ability to access your school email for safeguarding purposes.

Acceptable Use Policy Agreement

I understand that I must use Woodbrook Vale School's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

- I understand that Woodbrook Vale School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to Woodbrook Vale School ICT systems (e.g. laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that Woodbrook Vale School ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- 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 Woodbrook Vale School ICT 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, unless I have permission to do so. Where these images are published (e.g. on the Woodbrook Vale Website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies
- I will only communicate with students 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.

Woodbrook Vale School has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc) 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 school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- 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 ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult 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, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that Data Protection Policy requires that any staff or student 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 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 Woodbrook Vale School:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT 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. This could include a warning, a suspension, referral to Trustees and in the event of illegal activities the involvement of the police.

Aspire • Enjoy • Succeed

Acceptable Use Agreement
(Staff/Volunteer)
January 2023

I have read and understand the above and agree to use the school ICT 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.

Staff/Volunteer
Name……………………………………………………………………………………………

Signed…………………………………………………………………………………

Date…………………………………………………………………….

Appendix 3

Aspire • Enjoy • Succeed

Acceptable Use Agreement (Student)

January 2023

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital 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.

Woodbrook Vale School will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

This policy applies to any device in school. It applies across the whole network and includes Wi-Fi.

Woodbrook Vale School carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Woodbrook Vale School can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the internet is closely monitored by the school, logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device.

The school email system is provided for educational and business purposes, where required the school has the ability to access your school email, for safeguarding purposes and should a management requirement necessitate it.

Acceptable Use Policy Agreement

I understand that I must use Woodbrook Vale School ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that Woodbrook Vale School will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, 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 be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand Woodbrook Vale School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use Woodbrook Vale School systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I will appreciate that others may have different opinions.
- I will not take images of anyone in school unless instructed to do so by a member of staff and using a school device.
- I will not distribute images taken in school on a school device.

I recognise that Woodbrook Vale School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of Woodbrook Vale School:

- I keep my mobile devices switched off and in my bag. I accept that this only permitted for my safety when travelling to and from school. It is not permitted for any other purpose.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, 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 install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites when in school.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that Woodbrook Vale School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images, use of social media to be defamatory towards the school, students or members of staff or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Woodbrook Vale School
Acceptable Use Agreement
(Student)
January 2023

This form relates to the student Acceptable Use Agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use Woodbrook Vale School systems and devices (both in and out of school)
- I use my own equipment out of Woodbrook Vale School in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Name of Student: ……………………………………………………………………………

Tutor Group: …………………

Signed by Student: ………………………………………………………………………….

Signed by Parent: ……………………………………………………………………….….

Date: ………………………….