Online Safety Policy	
Independent School Standards: paragraphs 7 and 34	
Policy content: ● Usage, filtering and monitoring of the internet ● Managing and storing personal data ● Managing online safety incidents.	
Latest ratification by Trustees:	Sept 2023
Next review by Trustees:	October 2024
Latest Update:	August 2023
Links:	Safeguarding policy Complaints policy Data Protection policy Social media policy

Online safety policy

This policy is part of the school's statutory safeguarding policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

Appendices

1. Introduction and overview

1.1. Objectives

- To ensure all members of our school community understand and respect the guidelines set out in this policy in regards to all ICT, in order to safeguard and protect our young people and staff and enable them to use the internet and ICT (both in and out of school) safely and effectively.
- To ensure school staff monitor their own standards and practice, to work safely and responsibly with the internet and other ICT.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community.
- To ensure clear structures to deal with online abuse such as online bullying and incidents that may take place both within and outside of school.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with young people

1.2 Risk areas

Content exposure to inappropriate content	● Lifestyle websites promoting harmful behaviours ● Hate content including extremist material ● Inaccurate content validation ● False news and information ● Pornography or other sexually explicit or violent material
Contact	● Grooming (e.g. for sexual exploitation and/or radicalisation) ● Online bullying in all forms ● Social or commercial identity theft. including passwords
Conduct	● Aggressive behaviours such as online bullying ● Privacy issues, including disclosure of personal information ● Digital footprint and online reputation ● Health and wellbeing ● Sexting ● Sharing of inappropriate materials ● Copyright (little care or consideration for intellectual property)

1.3 Roles and responsibilities

1.3.1 Trustees

- Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. All online safety incidents and monitoring reports will be reported to the trustees by the co-headteacher.
- The safeguarding lead Dhama Sangarabalan has the responsibility for online safety and this role includes:
    - regular meetings with the data protection officer, Lee Cooper.
    - regular monitoring of online safety incident logs
    - regular monitoring of filtering/ change control logs
    - regular reporting to the trustees

1.3.2 Co-headteachers

- Have 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 data protection officer, Lee Cooper, who will update the co-headteachers with regular monitoring reports.
- The director Lucy Stephens, the trustee for safeguarding James Searjeant, and the data protection officer Lee Cooper, should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see 1.5 Handling Incidents flow chart below, and the relevant disciplinary procedures as set out in our safeguarding policy).
- Are responsible for ensuring that the data protection officer and the ICT technician receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- 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 to support those colleagues who take on important monitoring roles.
- Ensure that the school is registered with the Information Commissioner Office (ICO).

1.3.3 Designated safeguarding lead

- Take overall responsibility for data management and information security ensuring we follow best practice in information handling (see data policy).
- Take a leading role in establishing and reviewing the school's online safety policy and documents, as well as promoting an awareness and commitment to online safety throughout the school.
- Be trained in online safety issues and have a good awareness of the potential for serious child protection and safeguarding issues to arise from:
    - Sharing of personal data
    - Access to illegal/ inappropriate materials
    - Inappropriate online contact with adults/ strangers
    - Potential or actual incidents of grooming

    - Online bullying
- Liaise with school technical staff where appropriate.
- Communicate regularly with trustees to discuss current issues and review incident logs, ensuring all incidents are logged as a safeguarding incident.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Work with the data protection officer Lee Cooper to oversee any student surveys or feedback on online safety issues.
- Liaise with the local authority and relevant agencies; receive regular updates on online safety issues and legislation, and be aware of the potential for serious child protection concerns.

1.3.4 Data protection officer

- Lead the annual trustee meeting on online safety.
- Take day to day responsibility for online safety issues and take a leading role in establishing and reviewing the school online safety policies/ documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place (see 1.5 Handling incidents below) and to be a point of contact for any staff members who have questions or concerns about online safety.
- Work with the designated safeguarding lead to oversee any young people surveys or feedback on online safety issues.
- Liaise with school technical staff.
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments (see appendix E).
- Meet regularly with the co-headteachers to discuss current issues, review incident logs and filtering/ change control logs, attend relevant meetings/ update the trustees.

1.3.5 ICT technician/ provider

- Ensure the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Ensure the school meets required online safety technical requirements and any statutory online safety policy or guidance that may apply.
- Ensure users may only access the networks and devices through a properly enforced password protection policy.
- Ensures the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Ensure they are 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.
- Ensure that the use of the internet, network, remote access, email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and the Data protection officer for investigation.

- Ensure that monitoring software and systems are implemented and updated as agreed in the online safety policy.

1.3.6 Teaching and support staff

- Ensure they have an up to date awareness of online safety matters and of the current online safety policy and practices.
- Ensure they have read, understood and signed the staff acceptable use policy / agreement (AUP) (appendix D) which is then attached to their staff profile on Arbor.
- Ensure they report any suspected misuse or problem to the co-headteachers and the data protection officer immediately for investigation.
- Ensure all digital communications with young people and parents/ carers are on a professional level only and should be only carried out using official school systems.
- Ensure online safety issues are embedded in all aspects of the curriculum and other activities young people undertake, ensuring they understand and follow the online safety policy and acceptable use policies at all times.
- Ensure young people have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 young people should be guided to sites checked as suitable for their use; staff should follow the handling incidents process (1.5 below) to deal with any unsuitable material that is found in internet searches

1.3.7 Online safety group

- Includes the co-headteachers (designated safeguarding lead), the data protection officer, the ICT technician/ provider, the board of trustees.
- Takes responsibility for discussing issues regarding online safety and monitoring the online safety policy including the impact of initiatives.
- Members of the online safety group will assist the data protection officer with:
    - the production / review / monitoring of the school online safety policy and other related documents.
    - the production / review / monitoring of the school filtering policy and requests for filtering changes.
    - mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
    - monitoring network / internet / incident logs
    - consulting stakeholders – including parents / carers and the young people about the online safety provision
    - monitoring improvement actions identified through use of the 360 degree safe self-review tool

1.3.8 Young people

- Ensure they use the school digital technology systems in accordance with the student acceptable use agreement
- 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 in school; know and understand policies on the taking / use of images and on online-bullying.
- 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.

1.3.9 Parents/ carers

- Parents/ carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.
- The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website and through passing on any information about national or local online safety campaigns and literature.
- Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
    - digital and video images taken at school events
    - any parent Whatsapp groups or social media usage
    - their children's personal devices in the school

1.3.10 Volunteers

- Volunteers who access the school or the school systems as part of the wider school provision will be expected to sign a staff and volunteer user acceptable use agreement before being provided with access to the school systems.

1.4. Communication of policy

This policy will be communicated to staff and young people in the following ways:

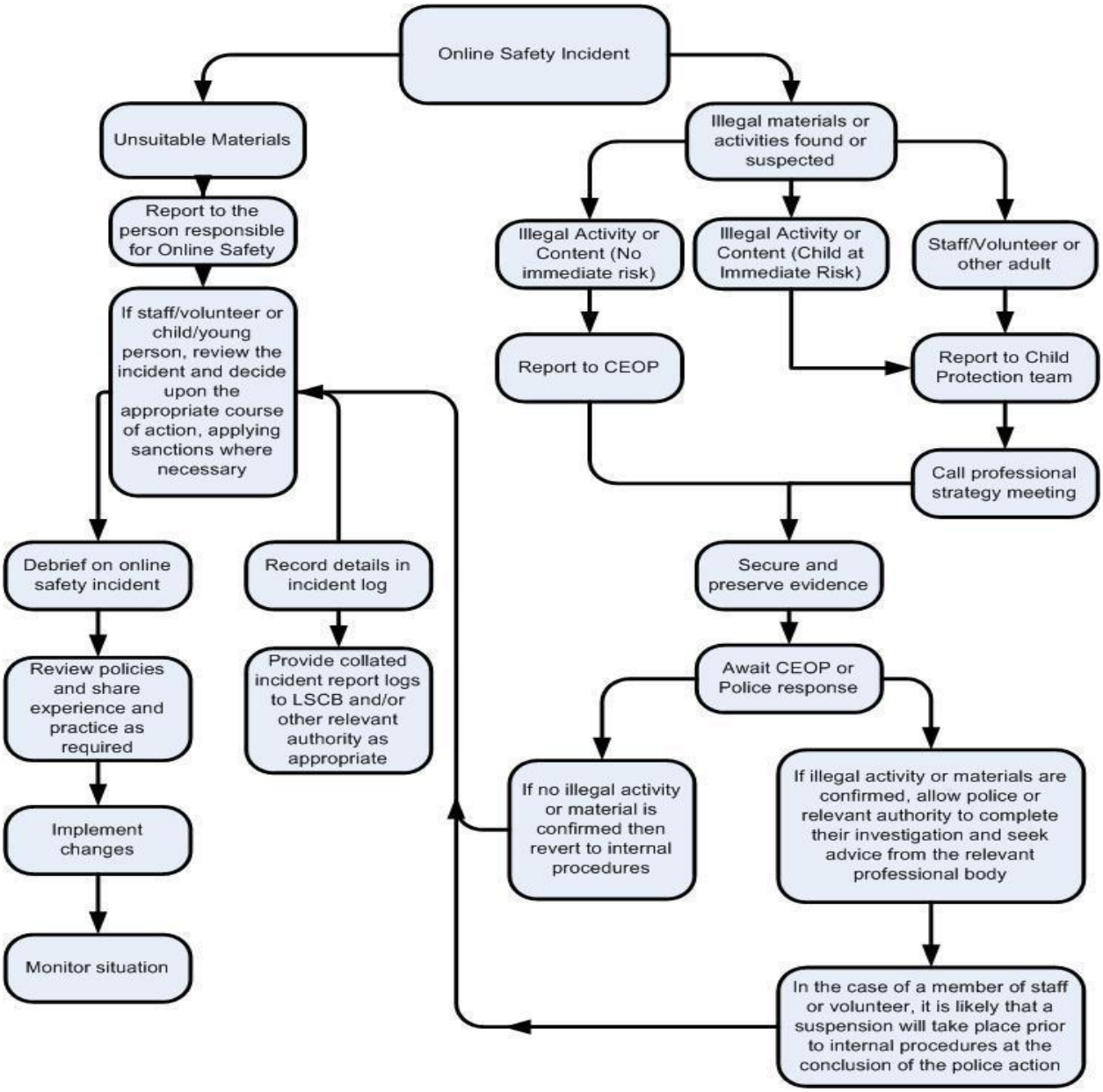
- Posted on the school website
- Included in the school induction pack for new staff.
- Regular updates and training on online safety for all staff and young people as part of online safety development days.
- Acceptable use agreements discussed with staff and young people at the start of each year.
- Acceptable use agreements to be issued to the whole school community, on entry to the school, signed and stored on the school database.

1.5 Handling incidents

The school will take all reasonable precautions to ensure online safety, however there may be occasions when staff need to manage incidents that involve the use of online services. Incidents may involve illegal or inappropriate activities.

1.5.1 Illegal incident procedure

If there is any suspicion that the website(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 this should be reported immediately to the Designated safeguarding lead, who will inform the police.



1.5.2 Other incidents procedure

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. Staff and young people are given information through training and lesson time about infringements in use and possible sanctions as outlined below.

In the event of suspicion, all steps in this procedure should be followed:

- The co-headteachers, the data protection officer and the designated safeguarding lead (if different), as well as a trustee should be immediately informed and involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- If the concern is about a co-headteacher the complainant should be referred to the chair of trustees and they will decide if the complaint should be referred to the LADO (as per our Safeguarding policy).
- Conduct this procedure 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. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the incident log (except in the case of images of child sexual abuse – see below)
- Once this process has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by the LA
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - **o** incidents of ‘grooming’ behaviour
    - **o** the sending of obscene materials to a child
    - **o** adult material which potentially breaches the Obscene Publications Act
    - **o** criminally racist material
    - **o** promotion of terrorism or extremism
    - **o** other criminal conduct, activity or materials

  Isolate the computer in question as best we can. Any change to its state may hinder a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites

were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

1.5.3 School actions and sanctions

If the school needs to deal with incidents that involve inappropriate rather than illegal misuse, it is still important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures as per appendix F below.

2. Education and curriculum

2.1. Education – young people

Whilst regulation and technical solutions are very important, their use must be balanced by educating young people to take a responsible approach. The education of young people in online safety and digital literacy 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 should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.
- The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities.
- Young people are taught critical literacy throughout the curriculum to enforce the need to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Young people are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Young people are supported to build resilience to radicalisation by providing a safe environment for debating controversial issues during PSHE lessons and helping them to understand how they can influence and participate in decision-making through our decision-making structures that are embedded in our school culture.
- Young people are 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 should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned; guide young people to sites checked as suitable for their use, and ensure familiarity with the Handling Incidents process in place for dealing with any unsuitable material found in internet searches.
- Where young people are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and follow the process if unsuitable material is found.

- It is accepted that from time to time, for good educational reasons, young people may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT technician can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be made in writing, with clear reasons for the need.

2.2 Education – Parents / Carers

Parents and carers play an essential role in the education of their children and in the monitoring and regulation of their children's online 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:

- Newsletters and policy documents on the website
- Reference to the relevant websites e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers
- Training and information events provided where required.

2.3 Education & training – staff and trustees

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

- A planned programme of formal online safety training will be made available to staff annually. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should participate in the annual training, and ensure that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Data protection officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff meetings and on INSET days.
- The Data protection officer will provide advice and guidance to individuals as required. Online Safety BOOST includes an array of presentation resources that the Data protection officer can access to deliver to staff **(**https://boost.swgfl.org.uk/)
- The chair of trustees, as well as those involved in health and safety and safeguarding,will take part in online safety training / awareness sessions. This will be offered through participation in school training, online training and information sessions for staff or parents

3. Managing the IT infrastructure

3.1. Internet access, security and filtering

3.1.1 Security

- It is The New School's responsibility to ensure we have all the online safety measures. This includes Sophos and Impero.
- The New School is responsible for ensuring that our school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. As a school we adhere to the following:
    - School technical systems will be managed in ways that ensure that the school meets recommended technical requirements as outlined in governmental guidance
    - There will be a 6 monthly review/ audits of the safety and security of school technical systems by the online safety officer using 360degree safe.
    - Servers, wireless systems and cabling are securely located and physical access restricted. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
    - We have a wireless network which is secured to industry, enterprise standard security level.
    - The school infrastructure and individual workstations are protected by up to date virus software.
    - Ensures all IT and communications systems have been installed professionally and are regularly reviewed to ensure they meet health and safety standards (see Health and Safety policy).
    - Has set-up the network with a shared work area for pupils and one for staff. Staff and young people are shown how to save work and access work from these areas.
    - The data protection officer, Lee Cooper is responsible for ensuring that software licence logs (see policy folder) are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
    - Access to personal data is securely controlled in line with the school's personal data policy and personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured through encryption software.
    - Does not allow any outside agencies to access the network remotely except where there is a clear professional need and then access is audited, restricted and is only through approved systems.
    - Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used only to support their professional responsibilities.
    - Mobile device security and management procedures are in place for school provided devices and/or where mobile devices are allowed access to school systems (see 3.6.1 mobile technologies).

- Supply or temporary staff (e.g. trainee teachers, supply teachers, or visitors) are given temporary access to the school system using a 'temp' username and password, after they have signed the AUA.
- Downloading of executable files and the installation of programmes on school devices is only ever done by the ICT technician or the external service provider.
- **School devices should be used for educational purposes only and should not be used or shared by family members.**

3.1.2 Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed.

- Internet access is filtered for all users. Illegal content (ie. child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Filtering systems enable us to use differentiated filtering for different groups and ages of users
- It allows us to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users where necessary for educational purposes. This is managed by the ICT technician and a request needs to be made in writing (see appendix E) and this will be signed off by two authorised approvers and logged for audit.
- The filtering decisions lie with the ICT technician and the data protection officer, who document the filtering policy, sign-off filter change requests, and review termly.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the data protection officer and the co-headteachers (see 1.5 Handling incidents).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- All users have a responsibility to report immediately to the Safeguarding Lead or the data protection officer any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
- Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.
- Young people will be made aware of the importance of filtering systems through the online safety education programme components delivered in the school curriculum. They will also be warned of the consequences of attempting to subvert the filtering system.
- Staff users will be made aware of the filtering systems through the Acceptable use agreement and online safety training.

- Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness training.

3.1.3 Monitoring

- School technical staff regularly monitor and record the activity of users on the school technical systems using Impero and users are made aware of this in the acceptable use agreement.
- Logs are maintained of access by users and of their actions while users are on the system, and our network monitoring system allows us to monitor all users at different times throughout the day, both incoming and outgoing activity, and enables us to respond to:

    - Bullying and threatening behaviour whether perpetrated by students or staff.
    - Abusive comments or offensive attitudes.
    - Inadvertent exposure to inappropriate web sites (pornography, violence, suicide).
    - Deliberate access to inappropriate websites.
    - Online gambling and shopping.
    - Un-moderated discussion forums and chat rooms.

- The monitoring system allows us to automatically monitor all screen content and keyboard activity in order to detect violations including pornography, profanity, violence, racism and drugs. We can also add user-specific words and phrases.
- If the system detects a violation or an attempt to access a forbidden file or URL, the screen is automatically captured and maintained within a secure database, providing our comprehensive audit log.
- An appropriate system is in place (see 1.5 Handling Incidents) for users to report any actual or potential technical incident to the Data protection officer, the ICT technician and the Safeguarding Lead.

3.1.4 Passwords

- All users have clearly defined access rights to school technical systems and devices and no user is able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- All users will be provided with a username and secure password by the ICT teacher, who will keep an up to date record of users and their usernames on our school management system Arbor.
- Users are responsible for the security of their username and password. The acceptable use agreements make it clear that passwords are to be kept private.
- If a password is compromised the ICT teacher should be notified immediately.
- For mobile devices, a secure pin is required to unlock the device at all times.
- Staff are required to use two factor authentication to further enhance security.

- The “master / administrator” passwords for the school ICT systems, used by the ICT teacher must also be available to the co-headteachers, and kept in a secure place on the school management system Arbor.

3.1.5 Email

- The New School provides staff with an email account for their professional use and makes clear personal email should be through a separate account.
- The school will contact the Police if one of our staff or young people receives an email that we consider is particularly disturbing or breaks the law.
- Users must immediately report to the data protection officer or the co-headteachers 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.
- We ensure that email accounts are maintained and up to date.
- Email users should be aware that email communications are monitored, therefore staff and young people should only use the school email system to communicate with others when in school or on school systems e.g. by remote access.
- We use a number of technologies to help protect users and systems from unsolicited, spam or infected emails.
- Staff are advised not to open any emails from an unknown sender or open any attachments they didn’t expect to receive. If they are unsure they must speak to the data protection officer before proceeding.

3.1.5.1 Young people

- Young people are taught about the online safety of using email both in school and at home.
- Young people will be provided with individual school email addresses for educational use.

3.1.5.2 Staff

- Staff only use the school email system for professional purposes.
- Never use email to transfer staff or student personal data. ‘Protect-level’ data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data or file must be protected with security encryption.
- Should never put personal or identifiable information (such as a young person’s name) in the subject line of an email.
- The language in which email is written is often less formal and more open to misinterpretation than a written memo or a formal letter, however correspondence via email from a school email account should adhere to standards expected of formal written communication.

- All school email is disclosable under the Freedom of Information and Data Protection legislation. Beware that anything you write in an email could potentially be made public.
- Emails can remain in a system or a period of time after you have deleted them. You must remember that although you may have deleted your copy of the email, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 and the Data Protection Act 1998.
- Agreement entered into an email can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.
- Email is primarily a communication tool, and email applications are not designed for keeping email as a record. Email that needs to be kept should be printed and added to the appropriate storage function e.g. does it form part of a young person's record? All attachments in email should be saved into an appropriate electronic filing system or printed out and placed in paper files.

3.2 School website

- The co-headteachers, supported by the board of trustees, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The school website complies with statutory DfE requirements for Independent Schools.
- The contact details on the website will be the school's address, email and telephone number. Staff or young people's personal information will not be published, unless consent has been given.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Student photographs published on the web, after parental consent has been given, do not have full names attached.
- We do not use young people's names when saving images in the file names or in the tags when publishing to the school website.
- The administrator account for the school website will be safeguarded with an appropriately strong password.

3.3 Online learning spaces

- If members of staff use online learning spaces, it is their joint responsibility to manage it (e.g. Google Classroom). Depending on their role, they may assign responsibility for different parts.
- All members of the school community are able to upload and share on these learning spaces where relevant.
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.

- In school, young people are only able to upload and publish within school approved cloud systems.

3.4 Social media
Refer to school social media policy.

- We follow guidance from the UK Safer Internet Centre to teach young people about social networking, acceptable behaviours and how to report misuse, intimidation or abuse. This is delivered through our online safety curriculum work.
- Young people/ staff and parents/ carers are required to sign and follow our acceptable use agreement.
- Parents/ carers are reminded about social networking risks and protocols through our parental acceptable use agreement and additional communications materials when required.
- Parents/ carers are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

3.5 CCTV and video recordings

3.5.1 CCTV operation

- We have CCTV installed (both internally and externally) in the school for the purpose of enhancing the security of the building and for staff and young person safety.
- The CCTV surveillance at the school is intended for the purpose of:
    - ○ Protecting the school buildings and school assets, both during and after school hours;
    - ○ Promoting the health and safety of staff, young people and visitors;
    - ○ Preventing bullying
    - ○ Reducing the incidence of crime and anti-social behaviour (including theft, vandalism);
    - ○ Supporting the police and other government agencies with enquiries
    - ○ Assisting in identifying, apprehending and prosecuting offenders; and
    - ○ Ensuring that the school rules and behavioural structures are respected so that the school can be properly managed.
- The CCTV system is owned and operated by the school, the deployment of which is determined by the co-headteachers.
- Some of the cameras in operation may have the ability to record sound for identification purposes.
- The operation and recordings are managed by the facilities manager and the HR manager.
- Recorded data is kept and stored on the school site. Recorded data will not be retained for longer than 14 days except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

- Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation and has the right to request access to those images in writing to the HR manager. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified (e.g. date, time, location). A log of all requested recordings is kept by HR. All staff are made aware of the restrictions in relation to access and disclosure of recorded images. We will not reveal any recordings or create any copies without appropriate permission.
- If the footage contains images of other individuals then the school must consider whether:
    - The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals.
    - The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained,
    - If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
    - The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.
- The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation and the GDPR.
- CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
- Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation and the GDPR.

3.6 Equipment and digital content

3.6.1 Mobile technologies

Mobile devices may be school owned or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

- All young people and staff should understand that the primary purpose of the use of mobile or personal devices in a school context is educational.
- Teaching about the safe and appropriate use of mobile technologies is an important part of the school's online safety education programme.
- Mobile devices brought into school are entirely at the staff member, student, parent or visitor's own risk, and are the responsibility of the device owner. The school

accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- School provided or approved mobile devices will be used as part of an approved and directed curriculum-based activity.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from the co-headteachers.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Student personal mobile devices, which are brought into school and are not used as part of a curriculum-based activity with consent from co-headteachers, must be turned off or put on silent, and stored out of sight on arrival at school. They must remain out of sight and either turned off or silent until the end of the day.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- All mobile device use is to be open to monitoring scrutiny and the co-headteachers are able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobile devices may be searched at any time as part of routine monitoring by request of the co-headteachers (see 3.6.3 search of devices).
- If a young person needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they should schedule this outside of their contact time with young people.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with young people, parents or carers is required, for instance for off-site activities.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide their own mobile number (by inputting 141) for confidentiality purposes.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Phones and devices must not be taken into examinations. Young people found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

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

3.6.2 Access, storage and syncing of school-owned devices

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes		Yes	
Internet only				Yes		
No network access						Yes

- For young people and staff devices, any access to software, apps and file use are managed by the ICT teacher and technician.
- When a staff or young person leaves and the device is returned, the staff member must remove their personal account so that the device can be factory reset and cleared for reuse.

3.6.3 Digital images and video

- Parental/carer permission for use of digital photographs or video involving their child forms part of the school AUA form when a young person joins the school.
- We do not identify young people in online photographic materials or include the full names of young people in the credits of any published school produced video materials/DVDs.
- Staff sign the school's online acceptable use policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of young people.
- If specific photos of young people (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.

1

- Young people are taught about how images can be manipulated and are asked to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their online safety scheme of work.
- Young people are advised to be very careful about placing any personal photos on any social online network space. They are taught to understand the need to maintain privacy settings so as not to make public any personal information.
- Young people are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location.
- We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- **In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/ carers comment on any activities involving other young people in the digital / video images.**
- Staff and volunteers are allowed to take digital or 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 without permission.
- Care should be taken when taking digital or video images that young people are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Young people must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images.
- Young people's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Young people's work can only be published with the permission of the young person.

3.6.4 Electronic devices – search and deletion

- With reference to the following guidance 'Screening, searching and confiscation – Advice for head teachers, staff and governing bodies' (2014 and updated January 2018), the co-headteachers have authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: ICT technician, HR manager, designated safeguarding lead
- The co-headteachers may authorise other staff members in writing in advance of any search they may undertake.

- Members of staff are made aware of the school's policy on 'Electronic devices – searching and deletion: at induction and at annual updating sessions on the school's online safety policy.
- Authorised staff have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.
    - Searching with consent - authorised staff may search with the young person's consent for any item
    - Searching without consent – authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for
- The authorised member of staff must have reasonable grounds for suspecting that a young person is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Reasonable grounds as determined by the co-headteachers, the data protection officer and the ICT technician together).
- The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search; it must be the possession of the young person.
- The authorised member of staff should take care that the search is not conducted in a public place.
- The authorised member of staff carrying out the search must be the same gender as the young person being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the young person being searched.
- There is a limited exception to this rule: Authorised staff can carry out a search of a young person of the opposite gender including without a witness present, but **only where they reasonably believe that there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.**
- The person conducting the search may not require the young person to remove any clothing other than outer clothing. Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves). 'Possessions' means any goods over which the young person has or appears to have control – this includes desks, lockers and bags.
- The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a Police officer) can do**.**
- Force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.
- The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident.
- If inappropriate material is found on the device it is up to the authorised member of staff and the co-headteachers to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or

whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:
    - child sexual abuse images (including images of one child held by another child)
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- The school provides support in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search through HR and our pastoral support teacher. Seeing such material can be most upsetting.
- The incident should then follow 1.5 Handling incidents policy.

4.0 Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

- Please refer to our data protection policy for more information
- We are registered with the Information Commissioner's Office (ICO).
- We have appointed a Data Protection Officer (DPO) – Lee Cooper, supported by the co-headteachers, who carry out Data Protection Impact Assessments (DPIA).

5.0 Strategic and operational practices

5.1 Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to logout of systems when leaving their computer, but also enforce lock-out after 30 minutes idle time.

5.2 Asset disposal

- Details of all school-owned hardware are recorded in a hardware inventory.
- Details of all school-owned software are recorded in a software inventory.
- Disposal of any 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.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

Reviewing and monitoring

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

- 360 degree safe Online Safety Self Review Tool

Appendices

Appendix A – Acceptable Use Agreement – Reception/ KS1
Appendix B – Acceptable Use Agreement – KS2/3
Appendix C – Acceptable Use Agreement – Parent/ Carer
Digital Image Agreement – Parent/ Carer
Cloud systems Agreement – Parent/ Carer
Appendix D – Acceptable Use Agreement – Staff/ Volunteer
Appendix E Record of reviewing devices and internet sites (responding to incidents of misuse)
Reporting log
Training needs audit log
Change of filtering log

Appendix A

Student / Pupil Acceptable Use Agreement Template – for Reception and KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): _____

Signed (parent): _____

Appendix B

Student / Pupil Acceptable Use Agreement Template – KS2

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.

For my own personal safety:

- I understand that the 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 that the 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 the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg 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 appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- 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 only use social media sites with permission and at the times that are allowed

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 the 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 or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.

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

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student: _____

Group / Class: _____

Signed: _____

Date: _____

Appendix C

Parent / Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They 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 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 parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that young people have good access to digital technologies to enhance their learning and will, in return, expect young people to agree to be responsible users. A copy of the student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name:_____

Student's Name:_____ _____

As the parent / carer of the above student, I give permission for my child to have access to the internet and to ICT systems at school.

- I know that the school has discussed the Acceptable Use Agreement with my child and my child has signed this.
- I understand that my child has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems.
- I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

- I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the school / academy is collecting personal data by issuing this form, it should inform parents / carers as to:

This form will be printed and kept on your child's record.
HR and the school staff will have access to this form
This form will be stored for the time your child is at The New School.
This form will be shredded in the school year following your child leaving The New School

Signed: _____

Date: _____

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Young people and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publically shared by any means, only your child's initials will be used.

The school will comply with the Data Protection Act and request parents/ carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/ carers comment on any activities involving other young people in the digital or video images.

Parents/ carers are requested to sign the permission form below to allow the school to take and use images of their children.

This form will be printed	The images
HR and the school staff will have access to this form and it will be stored on your child's record.	The images may be published on the school's social media accounts - Twitter, Facebook, Instagram or Linkedin; the school website; the local press or media, etc. (see relevant section of form below)
This form will be stored for the duration of your child's time at The New School.	The images will be stored on the school's secure system and HR will have access to these.
This form will be destroyed in the school year after your child leaves The New School.	The images will be stored for the duration of your child's time at The New School.
	The images will be destroyed in the school year after your child leaves The New School.
	If you require an image to be deleted, please make this request in writing to Rachel Mascia – HR Manager.

Digital / Video Images Permission

Parent/ Carers Name:_____

Student Name:_____

As the parent/ carer of the above student, I agree to the school taking digital / video images of my child / children.	Yes / No
I agree to these images being used:	
● to support learning activities.	Yes / No
● in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
● on the school's social media accounts (identified by initials only) ● on the school website (identified by initials only) ● in the press (identified by initials only)	Yes / No Yes/ No Yes/ No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: _____

Date: _____

Use of Cloud Systems Permission Form

The school uses Microsoft as the provider of our cloud service for students and staff. This permission form describes the tools and student responsibilities for using these services.

The following services are available to each young person as part of the school's online presence in Microsoft's cloud service.

Using Microsoft will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other students and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

This form is printed.	The data shared with the service provider
HR and the school staff will have access to this form and it will be stored on your child's record.	The data uploaded by young people includes all of their learning and project work. Their name will be used to generate an email address and a password.
This form will be stored for the duration of your child's time at The New School.	The data will be accessible by all school staff.
This form will be destroyed in the school year after your child leaves The New School.	Each student's data will be stored for the duration of their time at The New School.
	A request for deletion of the data can be made in writing to the HR manager Rachel Mascia.

Do you consent to your child to having access to this service?	Yes / No

Student Name: _____Parent / Carers Name:_____

Signed: _____Date: _____

Appendix D

Staff and Volunteer Acceptable Use Policy Agreement Template

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:

- 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 young people's 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 young people 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 rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, school mobiles 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 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 understand downloading of executable files and the installation of programmes on school devices is only ever done by the ICT technician or the external service provider.
- I understand school devices should be used for educational purposes only and should not be used or shared by members of family.
- 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 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 use formal written practises when communicating via email.
    - 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 (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured – I will only use initials of young people.
    - I will only use social networking sites in school in accordance with the school social media policy.
    - I will only communicate with young people and parents/ carers using official school systems. Any such communication will be professional in tone and manner.
    - I will only use school email or mobiles to communicate with parents/ carers and young people, unless in an emergency (please refer to school mobile phone policy)
    - I will not engage in any on-line activity that may compromise my professional responsibilities.

- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
    - When I use my mobile devices (laptops / tablets / 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 only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). 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 / 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 / academy 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:
        - 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 Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

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.

Staff / Volunteer Name: _____

Signed: _____

Date: _____

Appendix E

Record of reviewing devices / internet sites (responding to incidents of misuse)

Person/ Group involved: _____

Date: _____

Reason for investigation: _____

_____

_____

Details of first reviewing person

Name: _____

Position: _____

Signature: _____

Details of second reviewing person

Name: _____

Position: _____

Signature: _____

Name and location of computer used for review (for web sites)

_____

_____

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Incident reporting Log

Group: _____

Date	*Time*	*Incident*	*Action Taken*	
			What?	*By Whom?*

Training Needs Audit Log

Group: _____

Relevant training the last 12 months	**Identified Training Need**	**To be met by**

Change of filtering Log – needs to be submitted one week in advance

Group: _____

Teacher: ……..

Today's date	What is the change requested/ what sites need access?	Reason for request?	Date needed/ Sta time/ End time of filter change?

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Trustees on:	January 2020
The implementation of this Online Safety policy will be monitored by the:	Data protection officer Headteacher
Monitoring will take place at regular intervals:	Annually
The Board of Trustees will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed 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.	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LADO, Police

A hard copy of this policy may be requested from the school office during office hours.

<u>Privacy Statement</u>
Who we are: *The New School is the Data Controller.*
Why do we need your data: *Your and your young person's details are required by the school to facilitate your young person's admission to the school.*
What is the lawful basis for processing this data: *This information is necessary for the school's legitimate interests.*
Who will this data be shared with: *We will only share your data with third parties if we are legally obliged to do so.*
How long will we keep your data: *we will hold your data for as long as we have a lawful basis to process your data.*

Appendix F

Student Incidents	Actions / Sanctions								
	Refer to class teacher / tutor	Refer to Online Safety Officer	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction or investigation
Deliberately accessing or trying to access material that could be considered illegal (see list on unsuitable / inappropriate activities).		X	X		X	X		X	
Unauthorised use of non-educational sites during lessons	X								
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X						
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X						
Unauthorised downloading or uploading of files	X	X	X						
Allowing others to access school network by sharing username and passwords	X	X	X		X				
Attempting to access or accessing the school network, using another student's account	X	X	X		X				
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X		X	
Corrupting or destroying the data of other users	X	X	X			X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X						
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X			X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X						
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X		X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X					X	

Staff Incidents	Refer to headteacher	Refer to Online safety officer/ HR	Refer to trustee board	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X		X	
Inappropriate personal use of the internet / social media / personal email	X	X	X			X		
Unauthorised downloading or uploading of files	X	X	X			X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X		X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules	X	X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X		X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X					X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	X	X	X					X
Actions which could compromise the staff member's professional standing	X	X	X			X		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	X	X	X					X
Using proxy sites or other means to subvert the school's / academy' s filtering system	X	X	X		X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X		X	X
Breaching copyright or licensing regulations	X	X	X			X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X					X