Lydiard Park Academy

Online Safety Policy 2020-22

Why do we need an Online Safety policy?

In today's world, everyone interacts with technology on a daily basis. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but situations can occasionally arise which cause concern for young people or adults. Pupils can also unwittingly put themselves or others in danger.

Online Safety covers issues relating to electronic communications for both pupils and adults. It relates to usage both inside and outside of the Academy. It includes education for Academy stakeholders on risks and responsibilities and is part of the 'duty of care' which applies to everyone who works with children.

This Online Safety policy strikes a balance between controlling access to the Internet and technology and educating pupils and staff about responsible use. We must also accept that staff and pupils cannot be completely prevented from being exposed to risks, both offline and online.

Pupils must be empowered and educated so that they are equipped with the necessary skills to make safe and responsible decisions as well as able to identify when a concern must be reported. All members of staff need to be aware of the importance of good Online Safety practise in the classroom in order to educate and protect the children in their care. Members of

staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviour compatible with their role.

Breaches of an Online Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of wider Academy communities. It is crucial that all stakeholders are aware of the offline consequences that online actions can have.

- The Academy has appointed an Online Safety Coordinator.
- The Online Safety Policy and its implementation will be reviewed annually.
- Our Academy Policy has been agreed by the Senior Leadership Team and approved by governors.
- The Academy has appointed a member of the Governing Body to take lead responsibility for Online Safety.

The Interim Academy Online Safety Coordinator is: **Miss Mellia Robertson**

Teaching and learning

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

Internet use is part of the statutory curriculum and is a necessary resource for learning.

The Internet is a part of everyday life for education, business and social interaction. The Academy has a duty to provide pupils with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside of the Academy and need to learn how to evaluate online information and take care of their own safety and security.

- The purpose of Internet use in the Academy is to raise educational standards, to promote pupil achievement, to support the professional work of staff and enhance the Academy's management functions.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

Internet use benefits education:

- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.

- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Access to learning wherever and whenever convenient.

Internet use enhances learning:

- Academy Internet access is designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The Academy will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the Internet will be reviewed annually to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Pupils will learn how to evaluate Internet content.

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content. For example, researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is part of teaching and learning in every subject and will be viewed as a whole Academy requirement across the curriculum.

Information systems security

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

- Users must act reasonably - e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Servers are be located securely with physical access restricted.
- Virus protection for the whole network is installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

- The security of the Academy information systems and pupils data will be reviewed regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the Academy network will be regularly checked.
- The ICT strategic manager/ Network manager will review system capacity regularly.

email Management

Email is an essential means of communication for both staff and pupils. Directed email can bring significant educational benefits. Unregulated email can provide routes to pupils that bypass the traditional Academy boundaries.

In the Academy context (as in the business world), email should not be considered private and most Academies and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/ carers, pupils and other professionals for any official Academy business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- Pupils may only use approved email accounts for educational purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.

- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official Academy provided email accounts to communicate with pupils and parents/carers.
- Excessive social email can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper would be.
- The forwarding of chain messages is not permitted.

Published content

Publication of any information online should always be considered from a personal and Academy security viewpoint.

The Academy website will comply with the guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" images can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self portraits or images of pupils; work or of a team activity.

Images of pupils must not be published without the parent's or carer's permission. Pupils also need to be taught the reasons for caution in publishing personal information and images online.

- Images or videos that include pupils will be carefully selected and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Permission from parents or carers will be obtained before images/videos of pupils are electronically published.

Social networking, Social media and Publishing

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be aware of the potential risks of using social networking sites or personal publishing either professionally with pupils or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, multiplayer online gaming, chat rooms, instant messaging and many others.

- The Academy will control access to social media and social networking sites.
- Pupils will never be advised to give out personal details of any kind which may identify them and/or their location.
- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk-assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the Academy website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the Academy community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, harmful or defamatory.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of the Academy) will be raised with their parents/carers, particularly when considering pupils' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Academy Acceptable Use Policy.

Web filtering

Blocking strategies are used to prevent access to a list of unsuitable sites. Maintenance of this list is the responsibility of our filtering provider but teachers can also prompt to have unsuitable websites blocked by forwarding the address to the Network Management Team.

- *Dynamic content filtering is in place to examine pages and addresses for unsuitable words.*
- *Keyword lists filter search engine searches and web addresses for inappropriate results and web addresses.*
- *Website addresses are recorded and monitored. Reports can be produced to investigate pupil access.*

No filtering system is 100% effective. There are ways to bypass filters (such as using "proxy" websites, or using a device which is not connected to the network e.g. a mobile phone). Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using IT rooms access and that the Acceptable Use Policies are followed.

In addition, Internet Safety Rules will be displayed in all IT enabled rooms, and both children and adults will be educated about the risks online. There will also be an incident log to report breaches of filtering or inappropriate content being accessed. Parents will be informed of breaches where appropriate. Any material that the Academy believes is illegal must be reported to appropriate agencies such as the Swindon Police or CEOP.

- Academy broadband access includes filtering appropriate to the age level of our pupils.
- The filtering policy is continually reviewed.
- The Academy has a clear procedure for reporting breaches of filtering. All members of the Academy community will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the address will be reported to the Academy Online Safety Coordinator or the Network Management Team, who will then record the incident and escalate the concern as appropriate.
- Changes to the Academy filtering policy will be risk assessed by staff with educational and technical experience prior to changes and where appropriate with consent from the Senior Leadership Team.
- The Online Safety Officer will regularly check that the filtering methods selected are effective. These checks will be conducted with a Governor present. Notes will be made and sent to the Clerk of Governors.
- Any material that the Academy believes is illegal will be reported to appropriate agencies such as Swindon Police, IWF or CEOP.

How will videoconferencing be managed?

Videoconferencing enables pupils to see and hear each other between different locations. This "real time" interactive technology has many uses in education. Steps should be taken to ensure that only the expected participants have access to the video conversation.

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer
- Pupils will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non Academy site it is important to check that they are delivering material that is appropriate for your class.

Emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within Academy systems. Online communities can also be a way of encouraging a disaffected pupil to keep in touch.

The safety and effectiveness of virtual communities depends on pupils being trusted and identifiable. This may not be easy, as authentication beyond the Academy may be difficult as demonstrated by social networking sites and other online tools such as Facebook, YouTube, Skype and Twitter. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with Academy policy. Abusive messages should be dealt with under the Academy's behaviour and/or anti-bullying policies.

- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Academy Acceptable Use Policy.
- All learners receive this as part of the pupil induction pack.

Authorising Internet Access

- All staff will read and sign the "Acceptable Use Policy" before using any Academy ICT resources.
- Parents will be asked to read the Academy Acceptable Use Policy for pupil access (contained in induction pack) and discuss it with their child, where appropriate.
- All visitors to the Academy site who require access to the network or Internet access will be asked to read and sign an Acceptable Use Policy.

How will risks be managed?

As the quantity and breadth of information available through the Internet continues to grow, it is not possible to guard against every undesirable situation. The Academy will need to address the fact that it is not possible to completely remove the risk that pupils might access unsuitable materials via the Academy system.

- The Academy will take all reasonable precautions to ensure that pupils access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The Academy will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Swindon Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling of Incidents of concern

Online Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the Academy Designated Safeguarding Lead or Designated Deputy Safeguarding lead.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the Academy will determine the level of response necessary for the offence disclosed.

- All members of the Academy community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Designated Safeguarding Lead will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The Academy will manage Online Safety incidents in accordance with the Academy behaviour policy where appropriate.
- The Academy will inform parents/carers of any incidents of concerns as and when required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Academy will contact the Designated Safeguarding Lead and escalate the concern to the Police.

Handling Online Safety complaints

Parents, teachers and pupils should know how to use the Academy's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. Online Safety incidents may have an impact on pupils, staff and the wider Academy community both on and off site and can have civil, legal and disciplinary consequences.

A minor transgression of the Academy rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the Academy's behaviour policy. Potential child protection or illegal issues must be referred to the Academy Designated Child Protection Coordinator or Online Safety officer.

- Complaints about Internet misuse will be dealt with under the Academy's complaints procedure.
- Any complaint about staff misuse will be referred to the Principal.
- All Online Safety complaints and incidents will be recorded by the Academy, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the Academy to resolve issues.
- All members of the Academy community will need to be aware of the importance of confidentiality and the need to follow the official Academy procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the Academy's behaviour and child protection procedures.
- All members of the Academy community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the Academy community.

Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the Internet to deliberately hurt or upset someone" DCSF 2007.

Many young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, Academy staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident pupils will support innovation and safety.

There are a number of statutory obligations on Academies with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- *every Academy must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the Academy's behaviour policy which must be communicated to all pupils, Academy staff and parents.*
- *gives headteachers the ability to ensure that pupils behave when they are not on Academy premises or under the lawful control of Academy staff.*

Where bullying outside the Academy (such as online or via text) is reported, it should be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If Academy staff feels that an offence may have been committed they should seek assistance from the police.

For more information please read "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies" http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying
DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the Academy community will not be tolerated. Full details are set out in the Academy's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the Academy community affected by cyberbullying.
- All incidents of cyberbullying reported to the Academy will be recorded.

- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The Academy will take steps to identify the bully, where possible and appropriate. This may include examining Academy system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the Academy to support the approach to cyberbullying and the Academy's Online Safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Academy website

Our Virtual Learning Environment can offer a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate and sharing resources. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

- Impero (monitoring software) will be used by the Online Safety Officer to regularly monitor the usage of the VLE by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the VLE.
- Only members of the current pupil, parent/carers and staff community will have access to the VLE.
- All pupils will be mindful of copyright issues and will only upload appropriate content onto the VLE.
- When staff, pupils etc. leave the Academy their account or rights to specific Academy areas will be disabled.

- Any concerns about content on the VLE may be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - The material will be removed by the site administrator if the user does not comply.
    - Access to the VLE for the user may be suspended.
    - The user will need to discuss the issues with a member of SLT before reinstatement.
    - A pupil's parent/carer may be informed.
- A visitor may be invited onto the VLE by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.

Mobile phones and other personal devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA, MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other Internet enabled personal devices can be used to communicate in a variety of ways.

Mobile phones can present a number of problems when not used appropriately:

- *They are valuable items which may be stolen or damaged;*
- *Their use can render pupils or staff subject to cyberbullying;*
- *Internet access on phones and personal devices may allow pupils to bypass Academy security settings and filtering.*
- *They can undermine classroom discipline;*
- *Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.*

Mobile phones will be used in accordance with the Academy policy for managing these devices. Currently, during lessons they are expected to be off and stored in bags unless specific permission is given by a teacher for curricular use.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Academy community and any breaches will be dealt with as part of the Academy behaviour policy.
- Academy staff may confiscate a phone or device if they believe it is being used to contravene the behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is

suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought into Academy are the responsibility of the user. The Academy accepts no responsibility for the loss, theft or damage of such items. Nor will the Academy accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the Academy site such as changing rooms and toilets.

Pupils use of personal devices

- If a pupil breaches the Academy policy then they may be banned from bringing personal electronic devices into school.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use an Academy phone. Parents are advised not to contact their child via their mobile phone during the Academy day, but to contact the Academy office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Mobile Phone and devices will be switched off or switched to 'silent' mode during lessons. Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used for phone calls or other personal communication during teaching periods, unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

- Taking photographs of student work or other resources is acceptable, provided that pupils are not photographed.
- If a member of staff breaches the Academy policy then disciplinary action may be taken.

Communication of this policy to pupils:

- All pupils will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be established across the Academy to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An Online Safety module will be included in the PSHE, and ICT programmes covering both safe Academy and home use.
- Online Safety rules and copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- All pupils will receive instruction on home lessons taking place via MS TEAMS. Instruction to include having webcams switched to a blurred background and screen-printing of teachers or other pupils is not allowed. TEAMS will not take place on a one to one basis.

Communication of this policy to staff:

It is important that all staff feel confident to use new technologies in teaching and the Academy Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

ICT use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion about the Academy Online Safety Policy.

- The Online Safety Policy will be formally provided to and discussed with all members of staff during induction.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- The Academy will highlight useful online tools which staff should use with children in the classroom.

- All members of staff will be made aware that their online conduct out of the Academy could have an impact on their role and reputation within Academy. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The Academy may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an Appropriate Use Policy.

- Parents' attention will be drawn to the Academy Online Safety Policy in newsletters, the Academy prospectus and on the Academy website.
- A partnership approach to Online Safety at home in the Academy with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting Online Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an Online Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the Academy Acceptable Use Policy (in the induction pack) for pupils and discuss its implications with their children.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Pupil
Acceptable Usage Policy

- I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring Lydiard Park Academy into disrepute.
- I will not use language that could cause offence or stir up hatred against any ethnic, religious or other minority group.
- I will use appropriate language in all communications which go through the academy network.
- I will not attempt to visit websites that might be considered inappropriate or illegal.
- I will not receive, send or publish material that violates copyright law.
- I will not attempt to harm or destroy any equipment or the work of another user on the academy network.
- I will not trespass into other users' files or folders.
- I will not share my login details (including passwords) with anyone else. Likewise, I will never use anyone else's username and password.
- I will ensure that I log off after my network session has finished.
- If I find an unattended machine logged on – I will log it off immediately.
- I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
- I will not download and/or install any unapproved software, system utilities or resources from the Internet.
- I will ensure that if I think someone has learned my password then I will change it immediately and/or contact Miss Robertson.
- I realise that files held on the school network will be regularly checked by Miss Robertson or other members of staff.
- I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to Miss Robertson.

Online Safety Officer: Miss M Robertson
Robertsonm@lydiardparkacademy.org.uk

COVID-19 Remote Learning

Leadership Oversight and Approval

1. Remote learning will only take place using Microsoft TEAMS with work posted on line through Show My Homework. MS TEAMS has been assessed and approved by the Principal, Mr Pearson and the Senior Leadership Team.
2. Staff will only use Lydiard Park Academy specific, approved professional accounts with learners.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Mr David Williams, Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible e.g. a LPA laptop.
3. Online contact with learners will not take place outside of the operating times as defined by SLT:8am - 6pm
4. All remote lessons will be formally timetabled; a member of SLT, DSL and/or head of department is able to drop in at any time.
5. Live streamed remote learning sessions will only be held with approval and agreement from the Principal or a member of SLT.

Data Protection and Security

1. All remote learning and any other online communication will take place in line with current LPA confidentiality expectations as outlined in the Trust Data Protection policy.
2. Recording of lessons will be on the discretion of the Principal and SLT. If recording is to take place all participants will be made aware.
3. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
4. Only members of LPA community will be given access to MS Teams.
   Access to MS Teams will be managed in line with current IT security expectations such as:
    - Using strong passwords.
    - Logging off or locking devices when not in use.

Session Management

1. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - Language expectations
    - Disabling/limiting chat.
    - Staff not permitting learners to share screens
    - Meetings are invite only by class code.
2. When live streaming with learners:

- contact will be made via learners' LPA provided email accounts and logins.
- staff will mute/disable learners' videos and microphones. Learners can be unmuted if answering a question.

3. Live 1 to 1 sessions will only take place with approval from the Principal or a member of SLT.
4. A pre-agreed invitation email, detailing the session expectations, will be sent to those invited to attend. Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
5. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour Expectations

1. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
2. All participants are expected to behave in line with the existing LPA behaviour policy and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff or pupils will not take or record images for their own personal use.
3. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
4. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
5. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

1. Participants are encouraged to report concerns during remote session.
2. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the learners tutor and Head of Year.
3. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
4. Any safeguarding concerns will be reported to Mr David Williams, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Lydiard Park Academy Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: ……..……..

Date…….