Arts & Media School
ISLINGTON

ARTS & MEDIA SCHOOL ISLINGTON GENERAL ICT AND E-SAFETY POLICY

Our ICT and E-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. This E-Safety Policy has been agreed by the senior management team. It will be reviewed annually.

Learning and Teaching Context

Information and communication technology (ICT) prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. Our aim is to teach pupils to use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. We want our pupils to learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning; with pupils being able to make informed judgments about when and where to use ICT to best effect, and consider its implications for home and work both now and in the future.

We interpret the term 'information communication technology' to include the use of any equipment which allows users to communicate or manipulate information (in the broadest sense of the word) electronically. ICT is a tool for learning and the key for raising standards across the curriculum.

Aims

The overall aim for ICT is to enrich learning for all pupils and to ensure that teachers develop confidence and competence to use ICT in the effective teaching of their subject enabling all learners to:

- Use ICT with purpose and enjoyment
- Develop the necessary skills to exploit ICT
- Become autonomous users of ICT
- Evaluate the benefits of ICT and its impact on society
- Reach the highest possible standards of achievement
- Develop their ICT capability and understand the importance of information and how to select and prepare it
- Develop their skills in using hardware and software so as to enable them to manipulate information
- Develop their ability to apply ICT capability and ICT to support their use of language and communication
- Explore their attitudes towards ICT, its value for themselves, others and society, and their awareness of its advantages and limitations
- Develop good Health and Safety attitudes and practice

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school. Where necessary and appropriate the community police will be informed.

The School Curriculum

Children arrive in school with variable ICT experiences; the systems and software may be different to what they know. However, we view all prior achievements as an advantage and aim to build on them. ICT capability is delivered within all subjects in every year group, boosted by cross-curricular ICT projects and activities. This is highlighted in the school ICT plan and in subject plans. The following list provides some examples of ICT skills and applications utilised:

- Using ICT to present information
- Exploring rules and investigating data
- Creating, processing and viewing text, images and video
- Control, input, process and output
- Databases and data handling
- Desktop publishing
- Presentation software (PowerPoint)
- Internet
- Emailing
- E-Safety

In Key Stage 3 ICT is taught as a discreet lesson and through cross curricular activity in the entire range of subjects we offer.

In Year 10 and 11 ICT is taught through the Computer Science and ECDL specifications.

Curriculum Enhancement

Children with a computer at home are encouraged to use it for educational benefit and parents are offered advice about what is appropriate. All pupils are provided with access to an online environment (Google for Education) which facilitates access to their schoolwork at any time, wherever they have access to a computer and an internet connection.

The school recognises the advantages of the use of ICT by children with special educational needs and every effort is made to equip our system to meet their needs.
Staff should structure their electronic teaching materials with consideration to learning difficulties and any associated computer operating systems as required.

Health and Safety/Security

Children are encouraged to log computers off and prepare them for use by the next user. They have chairs of the correct height, eyes level with the top of the monitor screen, and are encouraged to sit comfortably and use both hands for the keyboard. Children will also be made aware of the correct way to sit when using the computer and the need to take regular breaks if they are to spend any length of time on computers.

Portable equipment will be checked annually and computers three-yearly under the Electricity at Work Regulation 1989. The Health and Safety at Work Act (1 January 1993), European Directive deals with requirements for computer positioning and quality of screen. This directive is followed for all administration staff. Whilst this legislation only applies to people at work we seek to provide conditions for all learners.

Each computer system has individual secure access to the management system. The files and network system are backed up regularly. The virus checker and filtering meet industry standards via the London Grid for Learning connection.

Copyright and Licensing

All software loaded on school computer systems must have been agreed with the person in charge of ICT. Personal software of learners and staff should not be loaded on the school system unless permission has been granted. We respect intellectual ownership of software. Copyright, Design and Patents Act (1988) The Act protects a wide range of work, both written and computer based, including:

- Copying Software
- Copying or Downloading music
- Copying images or photographs from the Web
- Copying text from web pages

Arts and Media School Islington

E-Safety Policy covering the Internet, School Network and Email

The Green Paper *Every Child Matters*[2] and the provisions of the *Children Act 2004*[3] , *Working Together to Safeguard Children*[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via social networks, websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings. This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks.

Overview of the technologies involved

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The World Wide Web
- E-mail
- Instant messaging often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (notably Facebook)
- Video broadcasting sites
- Chat Rooms
- Gaming sites including networked gaming sites
- Music download sites
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications
- On-line learning resources.

Whole school approach to the use of ICT

Creating a safe ICT learning environment includes three main elements at Arts and Media School Islington:

- An effective range of well managed technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive E-Safety education programme for pupils, staff and parents

Roles and Responsibilities

Role	Key Responsibilities
Head teacher Susan Service	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.
Online Safety Co-ordinator – Anban Naidoo Designated Child Protection Lead – Janina Morgan	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be

	aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety) Flora Goldhill	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities
Network Manager/technician - RM managed service	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Data and Information (Asset Owners) Managers (IAOs)	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
LGfL Nominated contact	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • To ensure that personal data is kept secure.
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. This practice is being implemented. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology

	Exit strategy • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually. This practice is being implemented. Student Acceptable use Policy will also be included in student diaries in 2017-18. • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and 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 • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their children. This practice is being implemented. • to consult with the school if they have any concerns about their children's use of technology • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school. This practice is being implemented. • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

All staff should be familiar with the school's Policy including:

- Safe use of school network, equipment and data
- Safe use of Internet including use of Internet-based communications services, such as instant messaging and social networks
- Safe use of E-mail
- Safe use of digital images and digital technologies, such as mobile 'phones and digital cameras
- Publication of pupil information/photographs and use of website
- E-Bullying or cyberbullying procedures
- Their role in providing E-Safety education for pupils

Using the school network equipment and data safely

Arts and Media School Islington:

- Ensures staff read and sign that they have understood the school's E-Safety Policy. Following this, they are set-up with internet and email access and can be given an individual network login username and password
- Provides pupils with a class and/or individual network login usernames and email addresses and passwords
- Makes it clear that staff and pupils must keep their individual login username and password private and must not leave them where others can find them
- Makes clear that pupils should never be allowed to logon or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network
- Makes clear that no-one should logon as another user – if two people log on at the same time this may corrupt personal files and profiles
- Confidential data is kept on the shared drive and is only accessible to staff members. Therefore, it is essential they log off or lock their computers (windows key +L)
- Each pupil and staff member has their own My Documents and is responsible for maintaining their own files
- Has set up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off or lock computers when they have finished working or are leaving the computer unattended
- Where a user finds a logged on machine, we require them to always log off and then log on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they **do** switch the computers off at the end of the day and especially on a Friday afternoon
- We requests that projectors are turned off at the end of each day

Managing the Internet safely

Why Internet use is important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and the government's E-learning strategy as well as a necessary tool for staff and pupils

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and meet rigorous standards including filtering appropriate to the age of pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear training in Internet use
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Education Programme

Arts and Media School Islington:

- Fosters a 'No Blame' environment which encourages pupils to tell a teacher/responsible adult immediately if they encounter any material which makes them feel uncomfortable.
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or E-Safety Co-ordinator.
- Ensures pupils are taught how to evaluate Internet content and to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Ensures pupils and staff know what to do if a cyberbullying or other E-Safety incident occurs

Authorising Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- All pupils must read and sign the Acceptable Use Agreement for ICT Use before using any school ICT resource
- Parents will be asked to sign and return the E-Safety Agreement Form
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn
- Throughout the school pupils' access to the Internet will be through adult supervised activity to specific, approved online materials
- Teachers will have access to pupil e-mails and related internet files for monitoring and assessment.

Internet access and information security

Arts and Media School Islington:

- Maintains broadband connectivity through the London Grid for Learning (LGfL)
- Ensures virus protection will be updated regularly
- Uses class log-ins and/or individual log-ins for pupils, staff and visitors

We use the LGfL filtering system which blocks sites which fall into categories such as pornography, race hatred, gaming, sites of an illegal nature; and which informs staff and pupils that they must report any failure of the filtering systems directly to the *(system administrator/teacher/Mr A Naidoo - the school's E-Safety Coordinator).* Our system administrators report to LA/LGfL where necessary.

This school will:

- Block all chat rooms and social networking sites known to us except those which are part of an educational network or approved learning platform.
- Use Blocking strategies prevent access to a list of unsuitable sites.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate pupil access.

School Website

http://www.artsandmedia.islington.sch.uk/

- Is the official site with main contact details, prospectus information and other potential information which may pertain to and benefit the general public
- This website is the editorial responsibility of the Headteacher who ensures that the content is accurate and quality of presentation is maintained

Managing email safely

Pupils

- We only use LGfL 'Safemail' with pupils
- Pupils should only use the LGfL school domain e-mail accounts on the school system
- Pupils are introduced to, and use e-mail as part of the ICT schemes of work and given guidance on safe and acceptable use and reporting procedures
- Pupils must keep their logins and passwords secret

Staff

- Staff can use the LGfL/school domain e-mail accounts or web-based e-mails for professional purposes or for legitimate personal uses deemed 'reasonable' by the Headteacher and Governing Body
- Staff are responsible for the content of all outgoing and incoming e-mail and will ensure acceptability of the content; and will handle any inappropriate material they receive in such a way as to help protect the school's ICT resources and shield others form harmful or offensive material
- Spam is unavoidable and issues about spam should be referred to the ICT Manager/E-Safety Co-ordinator straightaway. That person can inform people how to direct spam through a spam filter and will contact the ISP for further advice.

Managing digital images and video safely

- We do not use pupils' names when saving images in the file names
- From March 2011 we do not include the full names of pupils in the credits of any video materials/DVDs produced and published by the school.
- Staff sign the school's Acceptable Use Policy for ICT and the school's Code of Conduct policy refers to the use of mobile 'phones/personal equipment for taking pictures of pupils
- Pupils are taught about how images can be abused in their E-Safety education programme
- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school

Protection of Personal Data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.
The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Radicalisation and Extremism

The school's safeguarding policy which is available on our website (and in school, covers Radicalisation and Extremism.

Indicators of Vulnerability to Extremism and Radicalisation

1. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

2. Extremism is defined by the Government in the Prevent Strategy as: Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

3. Extremism is defined by the Crown Prosecution Service as:
   The demonstration of unacceptable behaviour by using any means or medium to express views which:
   - Encourage, justify or glorify terrorist violence in furtherance of particular beliefs.
   - Seek to provoke others to terrorist acts.
   - Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
   - Foster hatred which might lead to inter-community violence in the UK.

4. There is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

5. Pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff are able to recognise those vulnerabilities.

6. Indicators of vulnerability include:
   - Identity Crisis – the student / pupil is distanced from their cultural / religious heritage and experiences discomfort about their place in society.
   - Personal Crisis – the student / pupil may be experiencing family tensions; a sense of isolation; and low self-esteem; they may have dissociated from their existing friendship group and become involved with a new and different group of friends; they may be searching for answers to questions about identity, faith and belonging.
   - Personal Circumstances – migration; local community tensions; and events affecting the student / pupil's country or region of origin may contribute to a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy.
   - Unmet Aspirations – the student / pupil may have perceptions of injustice; a feeling of failure; rejection of civic life.
   - Experiences of Criminality – which may include involvement with criminal groups, imprisonment, and poor resettlement / reintegration?

- Special Educational Need – students / pupils may experience difficulties with social interaction, empathy with others, understanding the consequences of their actions and awareness of the motivations of others.

7. However, this list is not exhaustive, nor does it mean that all young people experiencing the above are at risk of radicalisation for the purposes of violent extremism.

8. More critical risk factors could include:

    - Being in contact with extremist recruiters.
    - Accessing violent extremist websites, especially those with a social networking element.
    - Possessing or accessing violent extremist literature.
    - Using extremist narratives and a global ideology to explain personal disadvantage.
    - Justifying the use of violence to solve societal issues.
    - Joining or seeking to join extremist organisations.
    - Significant changes to appearance and / or behaviour.
    - Experiencing a high level of social isolation resulting in issues of identity crisis and / or personal crisis.

8.2 Preventing Violent Extremism

Roles and Responsibilities of the Single Point of Contact (SPOC), The SPOC for Arts and Media School is Janina Morgan, who is responsible for:

- Ensuring that staff of the school is aware that Janina Morgan is the SPOC in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Maintaining and applying a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism, and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism.

- Raising awareness about the role and responsibilities of Arts and Media School in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Monitoring the effect in practice of the school's RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

- Raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism.

- Acting as the first point of contact within the school for case discussions relating to students / pupils who may be at risk of radicalisation or involved in terrorism.

How will E-safety complaints and incidents be handled?

The school will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for materials accessed, or any consequences of Internet access.

Pupils are given information about uses that are considered infringements in use and possible sanctions. Sanctions available include:

- Discussion with E-Safety Co-ordinator/ICT Manager/Headteacher
- Informing parents or carers
- Removal of Internet or computer access for a period (which could ultimately prevent access to files held on the system, including examination coursework)
- Referral to Local Authority/Police
- Other disciplinary action according to school's codes of conduct

Our E-Safety Co-ordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. All virtual bullying incidents are regarded and treated in exactly the same way as physical, 'real world' bullying incidents.

Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

How will staff, pupils and parents be informed of these E-Safety procedures?

- They will be fully explained and included within the school's E-Safety/Acceptable Use Policy. All staff will be required to sign the school's E-Safety Policy acceptance form
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate E-Safety/acceptable use form
- The school's E-Safety policy will be made available to parents through the school website.
- We will teach and encourage parents to understand the technology their child/ward uses and we promote the use of a home family ICT usage agreement
- Information on reporting abuse/cyberbullying etc will be made available by the school for pupils, staff and parents

E Safety Incident Form

Date of incident:	
Member of staff reporting incident:	
Url, (web address) of incident:	
Copy of screens/evidence saved to:	
Location of incident (room):	
Computer number if known:	
Details:	
Passed to:	
Action taken	

Use of the Internet (by pupils and staff) policy

Usually the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated information, at time they will be able to move beyond these to sites unfamiliar to the teacher.

The problems and issues that have been highlighted by the media concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules that are in place at the school for using the Internet
- Describe how these fit into the wider context of the discipline and **Personal, Social and Health Education** policies.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence. The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and carers.
- Offer guidance to staff about the use of social networking sites.

We feel that the best recipe for success lies in a combination of site-filtering, of supervision, and by fostering a responsible attitude in our pupils in partnership with parents.

Using the Internet to enhance education
The benefits include:

- Access to a wide variety of educational resources including libraries, art galleries and museums;
- Rapid and cost-effective world-wide communication;
- Gaining an understanding of people and cultures around the globe;
- Staff professional development through access to new curriculum materials, expert knowledge and practice;
- Exchange of curriculum and administrative data with the Local Authority and
- Social and leisure use;
- Greatly increased skills in Literacy, particularly in being able to research, read and appraise critically and them communicate what is important to others;
- The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons;
- All staff will review and evaluate resources available on web sites appropriate for the age range and ability of the pupils being taught.

Pupils' Access to the Internet

The School will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed towards every computer screen. Member of staff will be aware of the potential for misuse and will be responsible for explaining expectations of proper use to pupils.

Teachers will have access to pupils' emails and other Internet files generated in school, and will check these periodically to ensure that expectations of behaviour are being met.

Expectation of pupils using the Internet

- All pupils are expected to read and agree the **Pupil contract for safe computer and internet use (Appendix 1)**
- We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.
- Pupils using the World Wide Web are expected not to deliberately seek out any material on Extremism and Radicalisation. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.
- Pupils are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea of why they are using it.
- Pupils must not access other people's files unless they have permission to do so.
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- No program files may be downloaded from the Internet to the computer, to prevent corruption of data and to avoid viruses
- No programs on CD Rom or flash drive/memory sticks should be brought in from home for use in school. This is for both legal and security reasons. Homework completed at home may be brought in on a memory stick with the permission of the teacher, and may be virus scanned by the class teacher before use.
- No personal information such as phone numbers and addresses should be given out and no arrangements should be made to meet someone via the Internet/email, unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and may be denied access to Internet resources. They will also be subject to the general disciplinary procedures of the school.

Appendix 1 – Student Acceptable Use Agreement:

Arts & Media School ISLINGTON	**E-Safety Policy**	**Student Agreement Form**

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for appropriate school activities and learning and am aware that the school can monitor my internet use.
2. I will not bring files into school that can harm the school network or be used to circumvent school security tools.
3. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my key stage.
5. I will only e-mail or contact people I know, or those approved as part of learning activities.
6. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.
7. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.
8. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
9. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
10. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.
11. I am aware that some websites, games and social networks have age restrictions and I should respect this.
12. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

I have read and understand these rules and agree to them.

Name	
Signed	
Date	

Appendix 2 - Employee Agreement for the use of school technology:

Purpose

- To remain competitive, better serve our pupils and provide our employees with the best tools to do their jobs (hereinafter called 'the school') makes available to our workforce access to one or more forms of electronic media and services, including computers, e-mail, telephones, voicemail, fax machines, external electronic bulletin boards, wire services, online services, intranet, Internet and the World Wide Web.

- The school encourages the use of these media and associated services because they can make communication more efficient and effective and because they are valuable sources of information about educational issues, ideas, technology, and new products and services. However, all employees and everyone connected with the organisation should remember that electronic media and services provided by the school are school property and their purpose is to facilitate and support school business. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

- To ensure that all employees are responsible, the following guidelines have been established for using e-mail and the Internet. No policy can lay down rules to cover every possible situation. Instead, it is designed to express the philosophy of the school and set forth general principles when using electronic media and services.

Prohibited communications

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

1. Discriminatory or harassing;
2. Derogatory to any individual or group;
3. Obscene, sexually explicit or pornographic;
4. Defamatory or threatening;
5. In violation of any license governing the use of software; or
6. Engaged in for any purpose that is illegal or contrary to the school's policy or interests.

Personal use

The computers, electronic media and services provided by the school are primarily for educational use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal purposes during lunchtime, or alternative outside of the normal contracted hours, is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their educational purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

Access to employee communications

The school reserves the right to routinely gather logs for most electronic activities or monitor employee communications directly, e.g., telephone numbers dialed, sites accessed, call length, and time at which calls are made, for the following purposes:

1. Cost analysis;
2. Resource allocation;
3. Optimum technical management of information resources; and
4. Detecting patterns of use that indicate employees are violating school policies or engaging in illegal activity.

The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in

compliance with the law, this policy and other school policies.

Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

Under no circumstances should pupil–named data be transmitted over the Internet or email. The school has use of encrypted data systems for this purpose.

Software

To prevent computer viruses from being transmitted through the school's computer system, unauthorised downloading of any unauthorised software is strictly prohibited. Only software registered through the school may be downloaded. Employees should use virus trapping software on any home computer that is used to download planning or other information onto the school computers. Employees should contact the schools IT co-coordinator if they have any questions.

Security/appropriate use

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorisation has been granted by school management, employees are prohibited from engaging in, or attempting to engage in:

1. Hacking or obtaining access to systems or accounts they are not authorized to use.
2. Using other people's log-ins or passwords.
3. Breaching, testing, or monitoring computer or network security measures.

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Anyone obtaining electronic assess to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Encryption

Employees may use encryption software where applicable, which is supplied to them by the systems administrator for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a school computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

Participation in online forums

Employees should remember that any messages or information sent on school-provided facilities to one or more individuals via an electronic network - for example, Internet mailing lists, bulletin boards, and online services - are statements identifiable and attributable to the school.

The school recognises that participation in some forums might be important to the performance of an employee's job. For instance, an employee might find the answer to a technical problem by consulting members of a news group devoted to the technical area.

Violations

Any employee who abuses the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible disciplinary action, legal action.

Please note that this includes work related comments made outside of work.

Advice to staff on the use of social networking sites

- There have been many issues with Face book and other social networking sites in schools over the last couple of years.
- The internet is a public domain not a private one and staff in schools must be aware that information which they share and post is accessible to the public at large.
- It is therefore particularly important that staff do not name or discuss individuals – pupils, staff, parents or governors – on social networking sites. To do so would constitute a serious breach of confidentiality and data protection procedures.
- All staff in schools must also be aware that they are particularly vulnerable to accusations of inappropriate behaviour, even outside of school, and that these could potentially give rise to the involvement of the Teaching Agency and formal disciplinary procedures.
- All school staff, particularly teachers, risk exposure in the press and potential complaints to headteachers, governors and the Local Authority when information posted on the Internet suggests behaviour which compromises their position as role models to pupils.

The school offers the following advice to staff:

1. Ensure that you do not post any photographs on the Internet which could give cause for embarrassment.
2. Do not post any comments which could compromise your own integrity or which could bring the school, your colleagues, parents or the school community into disrepute.
3. Do not discuss school matters, including comments about pupils, staff, parents or governor on social networking sites.
4. Check that you are happy with the privacy levels on your pages and review these settings regularly.
5. You are very strongly advised **not to allow pupils to become 'friends'** on these sites. This is because it is deemed to be inappropriate to encourage out-of-school relationships with pupils and because of the nature of some of the likely content of material on sites used by adults.
6. All governors, teachers, teaching assistants and non-teaching staff will have an understanding of what radicalisation and extremism are is and why we need to be vigilant in school.
7. All governors, teachers, teaching assistants and non-teaching staff will know what the school policy is on tackling extremism and radicalisation and will follow the policy guidance swiftly when issues arise.
8. If a complaint is received about a member of school staff then this will be dealt with under the school's disciplinary procedures and in consultation with Islington Council's HR Schools' Team.

Appendix 3 - EMPLOYEE AGREEMENT ON USE OF E-MAIL AND THE INTERNET

(To be signed and a copy placed on staff file)

Arts & Media School ISLINGTON	**E-Safety Policy** **January 2016 Update**	**Staff Agreement Form**

I have read, understand, and agree to comply with the rules, and conditions governing the use of the School's computers, networks and telecommunications equipment and services. I understand that I have no expectation of privacy when I use any of the telecommunication equipment or services. I am aware that violations of this guideline on appropriate use of the e-mail, Internet systems and participation in social networking sites may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of e-mail, Internet systems and participation in social networking sites may reflect on the image of the School to our pupils, parents, governors and suppliers and that I have responsibility to maintain a positive representation of the school.

Signature .....

Date .....

Full Name .....
(Please print in capital letters)

Role .....