Author: AH for JPA
Date: September 2020
Review Date: September 2021

GOSFORTH GROUP

Jesmond Park Academy

Online Safety Policy

1. Purpose

This policy guidance aims to:

- Help everyone at Jesmond Park Academy understand their roles and responsibilities in ensuring the safe and acceptable handling/use of information technologies.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Academy community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

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

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Local Advisory Group

The Local Advisory Group has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Local Advisory Group will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety reports as provided by the designated safeguarding lead (DSL).

All Local Advisory Group members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet (Appendix 2)

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

3.3 The designated safeguarding lead

Details of the Academy's designated safeguarding lead (DSL) are set out in our Safeguarding and Child Protection policy.

The DSL takes lead responsibility for online safety in the Academy, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are recorded and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy's Behaviour and Rewards policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the Academy to the Principal and/or Local Advisory Group

This list is not intended to be exhaustive.

3.4 The ICT Managed Service

The ICT Managed Service is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at Academy, including terrorist and extremist material
- Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring the Academy's ICT systems on a daily basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are recorded, reported and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are recorded and reported to the DSL

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the internet (Appendix 2), and ensuring that students follow the Academy's terms on acceptable use (Appendix 1)

- Working with the DSL to ensure that any online safety incidents are recorded on CPOMS/SIMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy's Behaviour and Rewards policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

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

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

3.7 Visitors and members of the community

Visitors and members of the community who use the Academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In Key Stage 3 and 4, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report a range of concerns
- Evaluate internet content and be critically aware of materials they read online and be shown how to validate information before accepting its accuracy. Evaluating online materials is part of learning and teaching in every subject and will be viewed as a whole-Academy requirement across the curriculum.
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

The safe use of social media and the internet will also be covered in other subjects where relevant.

The Academy will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The Academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be promoted during parents' information/consultation evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

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

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the Academy will use all reasonable endeavors to ensure the incident is contained.

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

6.3 Examining electronic devices

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

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

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

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

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

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

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

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

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

8. Use of digital images, video conferencing, web cameras and other online meetings

We record data and information about students, staff and other resources. This makes us a 'data controller' and means we must adhere to a set of key principles when using data and information.

Photographing Children

The definition of personal data extends to photographs of children taken by Academy staff or others on their behalf (e.g. professional photographers). We seek informed consent from parents in relation to the taking and use of such photographs. We do this at the beginning of a new Academy year or on enrolment. Photographs are stored on secure drives and not left on devices.

Recommended Good Practice

The Data Protection Act is unlikely to apply in many cases where photographs are taken in Academies and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure.

Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

Photos taken for official Academy use may be covered by the Act and students should be advised why they are being taken.

Photos taken purely for personal use are exempt from the Act.

Examples

Personal use:

A parent takes a photograph of their child and some friends taking part in the Academy Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.

Grandparents are invited to the Academy nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Official Academy use:

Photographs of students or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.

A small group of students are photographed during a science lesson and the photo is to be used in the Academy prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.

Media use:

A photograph is taken by a local newspaper of a Academy awards ceremony. As long as the Academy has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

Video conferencing

Video conferencing can be used to enhance the curriculum by providing learning and teaching activities that allow students to link up with people in other locations and see and hear each other. We must ensure that staff and students take part in these opportunities in a safe and responsible manner:

All video conferencing activity is supervised by a suitable member of staff. Students do not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

Lesson Recording

We use specialist lesson recording equipment as a tool to share best teaching practice and to support professional development. We do not reveal any such recordings without the participants' permission.

9. ADVICE

Staff Advice

Ensure a clear professional basis for all communications with students – do not give students personal telephone numbers, mobile numbers and addresses. Only use School communication systems e.g. Microsoft Outlook, Teams, VLE/Frog

Social Networking Sites / Online Gaming

We very strongly recommend that staff do not allow access to their own personal areas or open lines of communications to students. It is very important that staff maintain professional relationships with students at all times and we feel that these may be compromised by allowing students access to personal information or photographs. However well we feel that we know students and however mature that we feel they are, it is always possible that messages may be misinterpreted by teenagers and relationships may be damaged as a result. Ensure you use appropriate privacy settings.

Email

It is essential that all communications with students are in connection with teaching and learning. Staff should only use their official Academy email address and it is recommended that students also use their Academy (rather than personal) email addresses when communicating with staff. The Academy e-mail is monitored and recorded.

Online publishing

It is unacceptable to publish any defamatory and/or knowingly false material about Gosforth Federated Academies, your colleagues and/or our students on social networking sites, 'blogs', 'wikis' or any other online publishing format.

Student Advice

The Academy computer network is for educational use and students should not abuse this system. When accessing the network, you must keep your password safe and you must not share your password with other people. You should not attempt to access the network area of other users or attempt to gain access to unsuitable information.

While attending Jesmond Park Academy, staff will guide you towards appropriate materials when accessing the Internet. Outside of Academy, you should take care regarding the use of the Internet, mobile phones and social media sites:

- You should be careful about who you share your personal contact details with. This includes email addresses and mobile phone numbers.
- You should take extra care when interacting with other people in chat rooms and online. These people may not be who they say they are.
- Do not give out personal information to people you do not know very well.
- Never agree to meet anyone who you have only had contact with online.
- To help keep you safe, share the details of the people you are communicating with, online, with your parents and friends.
- Take care if accessing social networking sites such as Facebook; Twitter; Instagram etc.
- Do not use social media sites to post offensive material or to make yourself vulnerable to the inappropriate actions of others.
- Avoid using mobile phones and text messages, in an inappropriate manner, which could be interpreted as cyber-bullying by the person receiving the communication.
- Take care - any photograph that you allow to be taken of you, or any image which you share online or via a mobile phone, can potentially be seen by a world audience via the Internet.

If you consider yourself, or another student, to be at risk from cyber-bullying or online-safety issues, please inform an adult – either at home or at the Academy. The designated staff with responsibility for Safeguarding are Chris Aitken, Clare Walker, Andy Costello, Dave Merrifield and Claire Munro.

10. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the Academy's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside the Academy. Any USB devices containing data relating to the Academy must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager Service.

Work devices must be used solely for work activities.

11. How the Academy will respond to issues of misuse

Applicable to all users of technology and connected systems:

Deliberate unlawful/inappropriate material must not be viewed/stored/distributed on any Academy system. This can include material which is in violation of any law/regulation or which can be considered by any reasonable person in its context to;

- be defamatory
- be violent
- be offensive
- be abusive
- be indecent or obscene
- be discriminatory
- incite hatred
- constitute bullying and/or harassment
- breach anyone's confidence, privacy, trade secrets or copyright
- promote extremism/extreme beliefs that are linked with violence to radicalise an individual/individuals to promote and act on extreme, violent beliefs

Particular care should be taken whenever you choose to use your own personal technologies in a work environment and ensure that other people, including children, are not able to see personal content which you would deem private or sensitive, keeping professional and private lives separate.

Where a student misuses the Academy's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the Academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

In the event of an unsuitable/inappropriate activity, the procedure detailed within the “Responding to incidents of misuse” (Appendix 3) should be followed.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues.

All staff members will receive training, covering relevant updates as and when required (for example through emails, e-bulletins and staff meetings).

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

13. Monitoring arrangements

The Staff can record behaviour and safeguarding issues related to online safety on CPOMS and SIMS. An incident report can be produced from CPOMS and SIMS.

This policy will be reviewed annually by AEH. At every review, the policy will be shared with the Local Advisory Group.

14. Links with other policies

This online safety policy is linked to our:

Safeguarding and Child protection policy

Behaviour and Rewards policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

Appendix 1:

Student Acceptable Use Policy

The Aim

The aim of the Acceptable Use Policy for students is to ensure that everyone is able to take advantage of the potential of ICT to support their learning in a responsible and safe manner.
To do this, students need to understand the rules and systems that are in place to protect them, to ensure that our Academy systems are secure and that no one is subject to bullying or abuse.

Responsibilities

All students are expected to act responsibly and show consideration for others when accessing the network, Office365, Virtual Learning Environment (VLE/Frog) and any other learning platform administered by Jesmond Park Academy or ICT Managed Service.

It is not acceptable to;

- Attempt to download or install any programs or games to Academy owned computers.
- Attempt to introduce a virus, or malicious code.
- Attempt to bypass network and systems security.
- Attempt to access or use another person's account.
- Attempt to gain access to an unauthorised area or system.
- Attempt to use any form of hacking or cracking software / system.
- Connect or install any networking device (router, switch, wireless access point etc.) to the network or via a computer.
- Connect or install any form of internet access device such as modem, broadband or internet enabled mobile phones directly to the physical network or via a computer.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence or anxiety to other users, or material which infringes copyright, or material which is unlawful.
- Engage in activities which waste technical support time and resources.
- Take food or drink of any kind into the ICT Rooms
- Wilfully damage or tamper with any network/ICT equipment

All networked computers in the Academy are monitored remotely which means that there is an electronic record of the sites you have visited and the files you have stored in your directory/Office365.

Security

- Each student is responsible for keeping their login secure and should not share it with anyone else
- No student is allowed to use a computer allocated to a member of staff.
- No users should log on as someone else, nor use a computer which has been logged on by someone else.
- Users should change their passwords regularly

- Users should also log off or lock the keyboard (using CTRL+ALT+DEL) when leaving a workstation, even for a short time.
- Access to the Internet is filtered to prevent access to inappropriate sites, and to protect the computer systems. Users should be aware that the Academy logs all internet use for all users.
- Users should ensure that they are not breaking copyright restrictions when copying and using material from the internet/World Wide Web.
- Legally, children are not allowed to take and store photographs of staff or other children without their written permission (in accordance with Data Protection Regulations)
- Users should be aware that the Academy has a right to access personal folders on the network. Privacy will be respected unless there is reason to think that the Student Acceptable Use Policy or Academy guidelines are not being followed.
- Email Accounts/Emails are automatically monitored and filtered and you should only email people you know.
- Never open an email attachment sent by someone you do not know or that you are concerned about
- Never reveal personal details about yourself, such as your address or telephone number, or arrange to meet someone you do not know in an email
- Messages must be phrased using acceptable language and in an acceptable tone
- Email messages sent to an external organisation should be checked and authorised before sending in the same way as a letter written on headed note paper

Use of other technology

- Tablets, memory cards, USB Storage Keys and anything else that can be used to store, transmit or manipulate data should be used responsibly, and in accordance with the Student Acceptable Use Policy.

Personal Laptops/Computers/Tablets/Smartphones

- Personal laptops/Computers/tablets/Smartphones can be connected to the Jesmond Park Academy Guest Wireless network only using the appropriate method.

Consequence/Sanctions Procedure(s)

Those who misuse the computer facilities and contravene the Student Acceptable

Use Policy will be subject to the appropriate consequence and/or sanctions as outlined in the Behaviour Policy.

IMPORTANT - Users of the network may be held liable for costs incurred for repair and/or replacement of equipment where the damage was caused by misuse.

I have read and understand Jesmond Park Academy Acceptable Use Policy

Signature: ___________________________________
Name: ______________________________________
Tutor Group: _________________________________
Date: _______________________________________

Appendix 2:

Staff ICT Acceptable Use Policy (Teaching, Support and Local Advisory Group)

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the Academy's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the Academy systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the Academy ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, tablets, email and social media sites.
- Academy owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT system manager (ICT Managed Service).
- I will ensure that any personal data of students, staff or parents/carers is kept in accordance with Data Protection regulations. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely.
- I will not keep professional documents which contain Academy-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the Academy Learning Platform/Cloud storage (Offoce365)/Management Information System (SIMS) to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the Academy computer system that is unrelated to Academy activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the Academy Online Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Professional as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the ICT System Manager (ICT Managed Service) where appropriate.
- I will not attempt to bypass any filtering and/or security systems put in place by the Academy. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any Academy related documents or files, then I will report this to ICT Support/Academy Business Manager as soon as possible.
- My electronic communications with students, Parents/Carers and other professionals will only take place via work approved communication channels e.g. via a Academy provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using Academy or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the Academy Code of Conduct and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the Academy, or Gosforth Federated Academies, into disrepute.
- I will promote Online Safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practice online either on or off site, then I will raise them with the Principal.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The Academy may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy. Where it believes unauthorised and/or inappropriate use of the service's information systems or unacceptable or inappropriate behaviour may be taking place, the Academy will invoke its disciplinary procedure. If the Academy suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

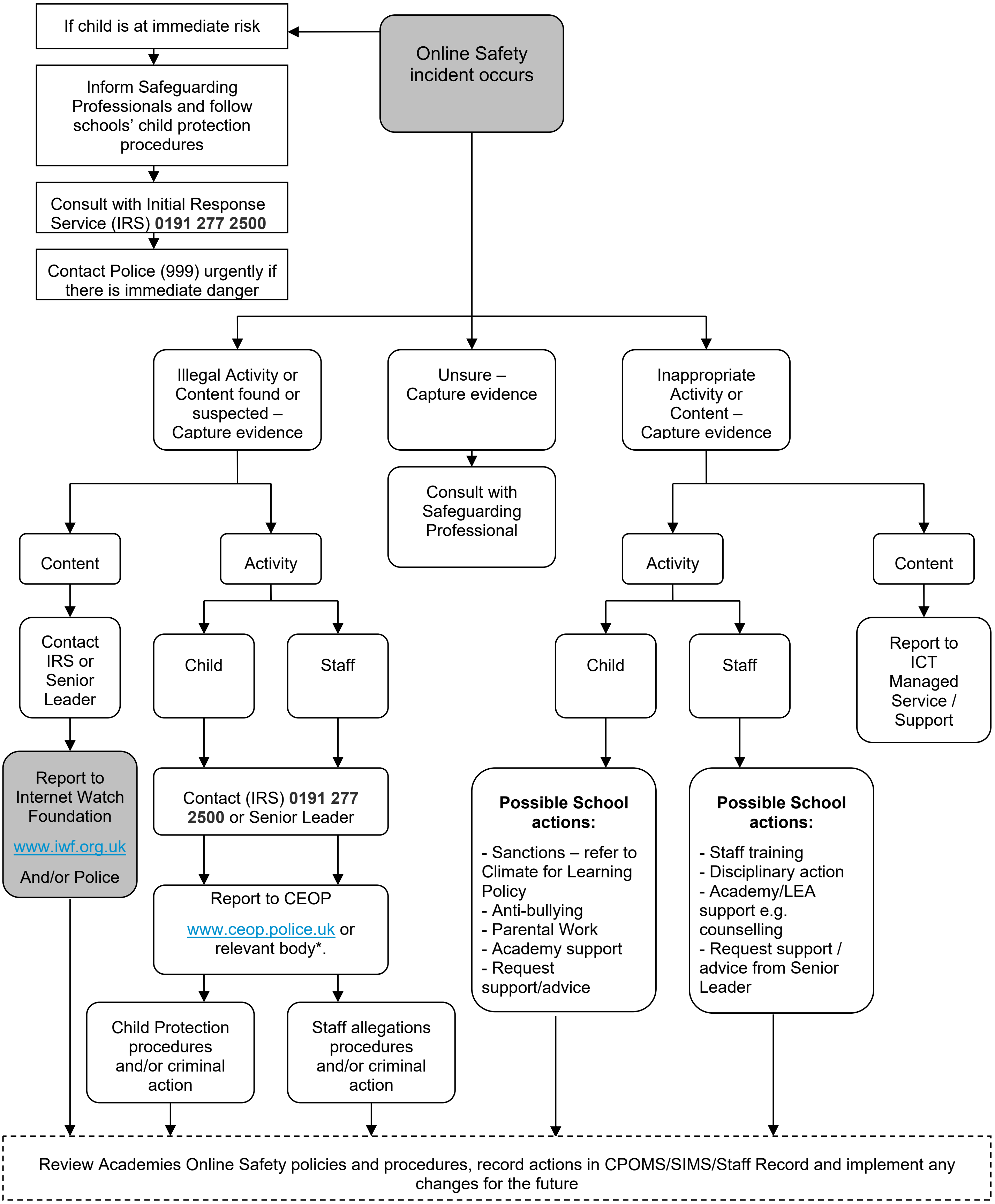
I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ___________________ Print Name: ___________________ Date: _________

Accepted by: ___________________Print Name: ___________________ Date: _______

Appendix 3

“Responding to incidents of misuse”



Online Safety incident occurs
If child is at immediate risk
Inform Safeguarding Professionals and follow schools’ child protection procedures
Consult with Initial Response Service (IRS) **0191 277 2500**
Contact Police (999) urgently if there is immediate danger
Illegal Activity or Content found or suspected – Capture evidence
Unsure – Capture evidence
Inappropriate Activity or Content – Capture evidence
Consult with Safeguarding Professional
Content
Activity
Contact IRS or Senior Leader
Child
Staff
Report to Internet Watch Foundation www.iwf.org.uk And/or Police
Contact (IRS) **0191 277 2500** or Senior Leader
Report to CEOP www.ceop.police.uk or relevant body*.
Child Protection procedures and/or criminal action
Staff allegations procedures and/or criminal action
Activity
Content
Child
Staff
Report to ICT Managed Service / Support
Possible School actions:
- Sanctions – refer to Climate for Learning Policy
- Anti-bullying
- Parental Work
- Academy support
- Request support/advice
Possible School actions:
- Staff training
- Disciplinary action
- Academy/LEA support e.g. counselling
- Request support / advice from Senior Leader
Review Academies Online Safety policies and procedures, record actions in CPOMS/SIMS/Staff Record and implement any changes for the future

***Reporting offensive content or Accessing help via External Organisations/Bodies**

Issue	Organisation/Body
Extremism and Radicalisation	UK anti-terrorist hotline on 0800 789 321 https://www.gov.uk/report-terrorism
Internet safety	Get safe online https://www.getsafeonline.org
Child sexual abuse imagery	Internet watch foundation https://www.iwf.org.uk/
Criminally obscene content	Internet watch foundation https://www.iwf.org.uk/
Cyber bullying	Childline - http://www.childline.org.uk/Explore/Bullying/Pages/Bullying.aspx Bullying - http://www.bullying.co.uk/
Grooming	Child exploitation and online protection centre - http://www.ceop.police.uk/
Anorexia and other eating disorders	Eating disorder association - http://www.nationaleatingdisorders.org/
Suicide help/support sites	Samaritans - http://www.samaritans.org/
	Bank safe online - http://www.financialfraudaction.org.uk/Consumer-fraud-prevention-advice-remote-banking.asp
Online scams	Trading standards - http://www.tradingstandards.uk/advice/
Online games	Video standards council - http://videostandards.org.uk/Home/
Hate crimes	True vision - http://www.report-it.org.uk/home

Recording/Capturing Evidence in the Event of an Online Safety Incident

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.
- Once this has been completed and fully investigated relevant Senior Leaders will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - extremism and radicalisation
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the Academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

September 2020

Date approved: ………………………………………………………………….

Signed: ………………………………………………………………….

September 2021

Date to be reviewed: ………………………………………………………………….