Emerson Park Academy

A SPECIALIST SPORTS COLLEGE

ENDEAVOUR
PERSEVERE
ACHIEVE

# ONLINE SAFETY POLICY

Approved: _____ by Board of Directors

Date: _____

Reviewed: June 2016 (J Galliano)

Next Review: June 2017

# Contents

## 1. Introduction and Overview

*Policy to support effective practice and embed Online Safety*

This policy should be read in conjunction with:

- EPA Acceptable Use Policy (Pupils)
- EPA Acceptable Use Policy (Staff)
- Social Media Policy
- Data Security Policy
- Child Protection Policy
- Behaviour Policy
- Anti-bullying Policy
- Anti Cyberbullying policy
- Preventing Radicalisation Policy

## Rationale and Scope

**The purpose of this policy is to:**

- Set out the key principles expected of all members of the Academy community at Emerson Park Academy with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist Academy staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole Academy community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the Academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

**The main areas of risk for our Academy community can be summarised as follows:**

### Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

### Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

### Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)
- Accessing or spreading extreme or radical material.

**Scope**

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

## Roles & responsibilities for online safety

**1. Responsibilities of the Head Teacher**

- To take ultimate responsibility for online safety issues and provision
- To be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance
- To take overall responsibility for data management and information security (SIRO) ensuring Academy's provision follows best practice in information handling
- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole Academy safeguarding.
- To delegate day-to-day responsibility to a member of SLT/Middle leadership as *Online Safety Co-ordinator (OSC)*
- To support the *Online Safety Co-ordinator*
- To receive regular monitoring reports from the Online Safety Co-ordinator
- To secure time, support and authority for the *online safety team (OST)* to function
- To secure funding for technical infrastructure and INSET/staff training
- To keep governing body informed and updated on the nature and effectiveness of the Academy's arrangements for online safety
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- 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 the Academy uses appropriate IT systems and services including, filtered Internet Service
- Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- To be aware of procedures to be followed in the event of a serious online safety incident
- To ensure Academy website includes relevant information.

**2. Responsibilities of Directors/Governors**

- To approve the Online Safety Policy and review the effectiveness of the policy on an annual basis
- To support the Academy in encouraging parents and the wider community to become engaged in online safety activities
- To elect a representative from the governing body to join the online safety team who will have the responsibility to attend OST termly meetings and review policies with the Online Safety Co-ordinator
- To develop an awareness of the issues and risks of using ICT and online technology in schools
- To develop an awareness of the benefits of engaging in online activities and using ICT in schools
- To develop an understanding of existing procedures and policies for maintaining a safe online learning environment
- To support the Head Teacher in formulating a plan/strategy to deal with media should a serious incident occur
- To ensure that the Academy has in place policies and practices to keep the children and staff safe online

**3. Responsibilities of the Online Safety Co-ordinator (OSC)**

- To take day to day responsibility for online safety issues and a leading role in establishing and reviewing the Academy's online safety policy/documents
- To assemble an Online Safety Team to review and advise on internet safety policies
- To promote an awareness and commitment to online safety throughout the Academy community
- To ensure that online safety education is embedded within the curriculum
- To maintain an overview of Online Safety activities across the Academy and support different departments/faculties
- To ensure that a log of all incidents relating to online safety breaches and monitoring of online activity is monitored within the Academy
- To make recommendations for review of policy and to update it annually or as required
- To organise appropriate meetings with the Head Teacher to discuss online safety issues and review progress
- To communicate regularly with SLT and the designated online safety representative from the governing body to discuss current issues, review incident logs and filtering/change control logs
- To inform the governing body on current online safety issues
- To liaise with Academy technical staff where appropriate
- To ensure that all academy staff are aware of the procedures that need to be followed in the event of an online safety incident
- To facilitate training and advice for all staff
- To oversee any pupil surveys / pupil feedback on online safety issues

- To liaise with the Local Authority and relevant agencies
- To remain abreast of online safety issues and legislation, and to be aware of matters that have the potential for serious child protection concerns.

**4. Network Manager and Network Support Staff**

- To support the Online Safety Co-ordinator
- To provide and maintain technical infrastructure and information on newly available technologies
- To manage the Academy's computer systems, ensuring:
  - Academy 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 Academy-owned devices
  - the Academy's policy on web filtering is applied and updated on a regular basis
- To ensure that the use of Academy technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Online Safety Co-ordinator/Head Teacher
- To ensure appropriate backup procedures and disaster recovery plans are in place
- To keep up-to-date documentation of the Academy's online security and technical procedures
- To remain abreast of online safety issues and technical information in order to effectively carry out their online safety role and to inform and update others as appropriate

**5. Head of BCI Faculty**

- To oversee the delivery of the online safety element of the Computing curriculum

**6. Subject Leaders and Heads of Faculty**

- To ensure pupils are properly supervised in ICT suites and in the use of online and communication technologies within their department/faculty
- To discuss general compliance, safety issues and good practise at faculty meetings
- To be familiar with protocols and procedures related to reporting and dealing with breaches in online safety

**7. Classroom teachers and LSA's**

- To embed online safety in the curriculum and within classroom practice
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended Academy 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 frequently review safety messages and respond appropriately
- To develop and maintain a high level of online safety awareness
- To report breaches of online safety to the relevant person.

**8. Heads of House**

- To contribute to the development of a safe ICT and online learning environment

- To ensure that Online Safety aspects are a big part of ensuring social welfare of pupils in each house
- To liaise with the OSC over the handling and investigation of Online Safety incidents within their house
- To impose sanctions within whole-Academy disciplinary framework appropriate for incidents of Online Safety breaches
- To support the OSC in maintaining/developing policies and procedures
- To act as mediators when called upon for ICT and Online Safety incidents which occur outside Academy e.g. bullying within chat rooms, creation of hate websites, etc.
- To attend OST termly meetings and contribute to the review and development of Online Safety policies
- To report breaches of online safety to the relevant person/agency.

**9. Head of Learning Support**

- To carefully consider the needs of pupils for whom they have responsibility and whether or not the Online Safety programme is appropriate or not, for example a pupil with autistic spectrum disorder will take messages very literally and could be persuaded to act upon them. Such a pupil is likely to need additional advice on safe behaviours and what he/she should never disclose to others
- To develop/maintain knowledge of Online Safety issues and how it affects children
- To liaise with parents/carers of pupils with special educational needs to ensure they are aware of the online safety issues their children may encounter outside Academy
- To co-operate with the Academy's child protection officer as necessary
- To attend OST termly meetings and contribute to the review and development of Online Safety policies
- To report breaches of online safety to the relevant person/agency.

**10. Child Protection Officer**

- To seek professional development on the safety issues related to the use of the internet and related technologies and how it relates to children
- To act as a key member of the Online Safety Team
- To take a proactive role in the provision for Online Safety education of pupils within the Academy
- To develop systems for supporting/referring on pupils to the OSC or relevant agencies as a result of breaches of the Online Safety policy within the Academy (eg Prevent Officer)
- To develop systems and procedures for pupils who self-refer and suspected victims
- To develop and maintain strategic partnerships with external agencies for Online Safety procedures
- To attend OST termly meetings and contribute to the review and development of Online Safety policies

**11. Data and Information (Asset Owners) Managers (IAOs)**

- To ensure that the data they manage is accurate and up-to-date
- To 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.

- To ensure that the Academy is registered with the Information Commissioner

**12. Pupils**

- To uphold policies related to acceptable use of the internet and communication technologies
- To develop safe and non-discriminating behaviours to guide themselves online
- To report any incident of ICT misuse, abuse and bullying to a responsible adult within the Academy
- To report any incident of radicalisation and extremism to a responsible adult within the academy.
- To seek immediate help and advice if/when they experience danger or are subjected to unnecessary abuse problems whenever they are online. Within Academy pupils should inform or report incidents/concerns to a responsible adult within the Academy community
- To communicate with their parents/carers about Online Safety issues and upholding all the rules for safe internet use at home

**14. Parents/carers**

- To read, understand and promote the Academy's Pupil Acceptable Use Agreement with their child/ren
- To consult with the Academy if they have any concerns about their children's use of technology
- To support the Academy in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the Academy's use of photographic and video images
- To support the Academy by ensuring that parents/carers endorse the relevant sections of the Pupils' Acceptable Use Policy agreement and Academy's use of photographic and video images agreements
- To read the advice and guidance provided by the Academy via Parent Pay Email and the website.

**15. External groups including Parent groups**

- Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within Academy
- To support the Academy in promoting online safety
- To model safe, responsible and positive behaviours in their own use of technology.

## The Online Safety Team (OST)

The OSC has formed an Online Safety team that will meet once a term to discuss the following:

- Review the Online Safety Policy, Pupil AUP, Staff AUP and Data Security Policy
- Review and evaluate the Internet Safety educational programs
- Process Policy updates
- Evaluate Internet Safety protocols so that incidents are responded to in an appropriate and consistent manner

The OST at Emerson Park Academy is:

Mr J Galliano (Online Safety Coordinator and Head of BCI Faculty)
Mrs C Crawley (Assistant Head Teacher)
Mr M Hope (Assistant Head Teacher)
Ms J Marsh (Child Protection Officer)
Mrs J Egleton (Head of Learning Support & Designated Teacher for Looked After Children)
Mrs S Hedges (Head of House)
Mr P Brickley (Head of House)
Mrs C Freeman (Head of House)
Mrs T Lindsey (Head of House)
Mr T Chowdhury (Network Manager)
Mrs B Sumbal (Curriculum Network Support)

### Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the Academy website/ Intranet / emailed to staff.
- Policy to be part of Academy induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole Academy community, on entry to the Academy.

### Handling Incidents:

- The Academy will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident other than when (or it is suspected that) a child's safety or welfare is at risk in which case the CPO MUST be informed first. (eg Sexual exploitation/radicalisation and extremism)
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Head Teacher, unless the concern is about the Head Teacher in which case the compliant is referred to the Chair of the Governing body

### Review and Monitoring

The online safety policy is referenced within other Academy policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, Social Media Policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the Academy
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by the Governing body. All amendments to the Academy online safety policy will be disseminated to all members of staff and pupils.

## 2. Education and Curriculum

As part of the education program for Online Safety and to further embed e-safety principles, discreet lessons on e-safety will be taught in Computer Science lessons in years 7 and 8 and across the age range in form classes and PSHE based lessons.

The Online Safety Coordinator will devise and implement an education program for pupils that will encourage them to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published and also inform them about the dangers of collaborating digitally and what to do and who to go to when things go wrong, both in Academy and out of Academy.

## Pupil Online Safety Curriculum

This Academy:

- has a clear, progressive Online Safety education programme as part of the Computing curriculum and PSHE education;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use Academy-approved systems and publish within appropriately secure / age-appropriate environments.
-

## Staff and Governing Body training

This Academy:

- will make regular training available to staff on Online Safety issues and the Academy's online safety education programme;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the Academy's Acceptable Use Agreements.

## Parent awareness and training

This Academy:

- will provide an induction talk on online safety for new Year 7 parents
- will provide online safety advice and guidance for parents on the Academy website

# 3. Expected Conduct and Incident management

## Expected conduct

In this Academy, all users:

- are responsible for using the Academy IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;

- understand the importance of adopting good online safety practice when using digital technologies in and out of the Academy;
- know and understand Academy policies on the use of mobile and hand held devices including cameras;

## Staff, volunteers and contractors

- know how to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know how to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

## Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the Academy's 'rules of appropriate use for the whole Academy community' are and what sanctions result from misuse.

## Incident Management

In this Academy:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the Academy are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the Academy's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the Academy;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

# 4. Managing IT and Communication System

## Internet access, security (virus protection) and filtering

This Academy:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;

- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- uses USO user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.

## Network management (user access, backup)

This Academy:

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote learning' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of Academy data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the Academy will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this Academy:

- Ensures staff read and sign that they have understood the Academy's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password
- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- 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 log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the Academy and/or connected to the network has up to date virus protection;

- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the Academy, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the Academy's network resources from remote locations by staff is audited and restricted and access is only through Academy/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This Academy uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other Academys;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted ;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

## Password policy

- This Academy makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the Academy should be notified immediately.
- All staff have their own unique username and private passwords to access Academy systems. Staff are responsible for keeping their password(s) private.
- We encourage staff to use STRONG passwords.
- We encourage staff to change their passwords into the MIS, LGfL USO admin site, at least once a year.
- We require staff using critical systems to use two factor authentication.

## E-mail

**This Academy**

- Provides staff with an email account for their professional use and makes clear that personal email should be through a separate account.
- We use anonymous or group e-mail addresses
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and .up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the Academy, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

**Pupils:**

- We use LGfL pupil email system which are intentionally 'anonymised' for pupil protection.

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in Academy and at home.

**Staff:**

- Staff will use LA or LGfL e-mail systems for professional purposes
- Access in Academy to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

## Academy website

- The Head Teacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The Academy web site complies with statutory DFE requirements;
- Most material is the Academy's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the Academy website;

## Cloud Environments

- Uploading of information on the Academys' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the Academy's online environment will only be accessible by members of the Academy community;

## Social networking

**Staff, Volunteers and Contractors**

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the Academys' preferred system for such communications.
- for the use of any Academy approved social networking will adhere to Academy's Social Media Policy.

**Academy staff will ensure that in private use:**

- No reference should be made in social media to pupils, parents/carers or Academy staff;
- Academy staff should not be online friends with any pupil. Any exceptions must be approved by the Head Teacher.
- They do not engage in online discussion on personal matters relating to members of the Academy community;

- Personal opinions should not be attributed to the Academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the Academy into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

**Pupils:**

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum and form period work.
- Pupils are required to sign and follow our pupil Acceptable Use Agreement.

**Parents:**

- Parents are reminded about social networking risks and protocols and countersign the parental section on our pupil Acceptable Use Agreement.
- Will be reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

## CCTV

- The Academy uses CCTV as part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted in the Academy. We will not reveal any recordings without appropriate permission.
- We use specialist lesson recording equipment (IRIS) on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

# 5. Data security

## Data Protection

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a Academy play or sports day. However, photographs taken for official Academy use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and parents should be advised why they are being taken.
Parental permission should be obtained before publishing any photographs, video footage etc. of pupils on the Academy website, in a DVD or in any other high profile public printed media. This ensures that parents are aware of the way the image of their child is representing the Academy; a printed copy of the specific image should be attached to this form.

## Strategic and operational practices

At this Academy:

- The Head Teacher will be the designated Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key Academy information (the Information Asset Owners) are. We have listed the information and information asset owners.

- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

### Technical Solutions

- Staff have a secure user area(s) on the network to store files and are encourage to password protect sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce screen lock-out after 10 minutes idle time.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all Academy-owned hardware will be recorded in a hardware inventory.
- Details of all Academy-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

## 6. Equipment and Digital Content

### Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into Academy are entirely at the staff member, pupils & parents or visitors own risk. The Academy accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into Academy.
- Mobile devices brought in to Academy are the responsibility of the device owner. The Academy accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- All mobile devices brought in by pupils will stored in their blazer inside pocket or bag during lesson time.
- Personal mobile devices will not be used during lessons or formal Academy time unless as part of an approved and directed curriculum-based activity with consent the class teacher.
- Pupil personal mobile devices, which are brought into Academy, must be turned off (not placed on silent) and stored out of sight on arrival at Academy. They must remain turned off and out of sight during lesson time.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members are permitted to use their phones during the Academy day but must use it responsibly and not during lesson time.
- All visitors are encouraged to keep their phones on silent whenever possible
- The recording, taking and sharing of images, video and audio on any personal mobile device should be avoided, except where it has been explicitly agreed by the Head Teacher. Such

authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Head Teacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

- The Academy reserves the right to search the content of any mobile devices on the Academy premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles could be accessed as part of a routine investigation in-line with union guidelines.
- If a pupil needs to contact his or her parents or carers, they should use a 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' use of personal devices

- The Academy accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil breaches Academy policy, then the device will be confiscated and will be held in a secure place in the Academy office. Mobile devices will be released to pupils, parents or carers in accordance with Academy policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- 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 personally-owned devices and will be made aware of boundaries and consequences.

## Staff use of personal devices

- Any permitted images or files taken in Academy must be downloaded from any handheld device including mobile phones and deleted in school before the end of the day.
- Staff should use their own mobile phones or devices in a professional capacity and will ideally use the Academy phone for contacting children, young people or their families within or outside of the setting.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff are encouraged not to use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and should use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a Academy-owned device, they should hide (by inputting 141) their own mobile number for confidentiality purposes.
- If a member of staff breaches the Academy policy then disciplinary action may be taken.

## Digital images and video

The use of images and video within the Academy must be safe and used responsibly.
The Online Safety Coordinator will oversee and authorise the Academy website's content and check suitability. Only the Head Teacher, Online Safety Coordinator and the ICT Technical Support Team have the authority to upload content into sections of our website.

Before content is uploaded to the Academy website the person uploading should ensure that the Academy is not infringing on copyright or intellectual property rights through any content published on the website.

Links to any external websites will be thoroughly checked by the Web Master before inclusion on our Academy website to ensure that the content is appropriate both to the Academy and for the intended audience.
The Academy will take care when using photographs or video footage of pupils on the Academy website. Group photographs rather than photos of individual children will be taken where appropriate.
To reduce the risk of inappropriate, unsolicited attention from people outside the Academy, names of individuals will never be used in photographs.

Whenever the Academy website is using a webcam it will be checked and monitored by the Online Safety Coordinator and/or the ICT Technical Support Team to ensure misuse does not occur accidentally or otherwise.

When showcasing Academy-made digital video work staff must take care to ensure that pupils aren't referred to by name on the video and that pupils' full names aren't given in credits at the end of the film. If showcasing examples of pupils work staff must use only their first names, rather than their full names.

It is very important that whenever images or video is used, pupils should be in suitable dress to reduce the risk of inappropriate use.

Staff should not use their personal phone or camera without permission e.g. for a Academy field trip. If personal equipment is being used it should be registered with the Online Safety Coordinator and a undertaking have to be signed that photographs will be transferred to the Academy network and will not be stored at home or on memory sticks and used for any other purpose than for Academy approved business.

**In this Academy:**

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the Academy agreement form when their daughter/son joins the Academy (or annually);
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published Academy produced video materials/DVDs;
- Staff sign the Academy's Acceptable Use Policy which includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the Academy web site, in the prospectus or in other high profile publications the Academy will obtain individual parental or pupil permission for its long term, high profile use
- The Academy blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;

- Pupils are advised to be very careful about placing any personal photos on any ‘social’ online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.