KADER ACADEMY

E–SAFETY POLICY

KADER ACADEMY

E–Safety Policy

CONTENTS

1 Introduction

1.1 At Kader Academy IT is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults.

2 Scope of the Policy

2.1 This Policy will apply to everyone in the school community and will be implemented by all staff employed by Kader Academy.

2.2 The Principal will report to governors on the operation of this policy. The document is subject to review as required.

3 Aim

3.1 The aim of this policy is to:

- Set out the key principles expected of all members of the school community at Kader Academy with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Kader Academy.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Ensure that all staff are aware of individual responsibilities relating to the safeguarding of children within the context of E-safety and know what to do in the event of misuse of technology by any member of the school community
- Set clear expectations of behaviour and/ or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross-referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations against adults who work with students.

3.2 The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/ self-harm/ suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (Self generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

4 Roles and Responsibilities

The Principal

4.1 It is the role and responsibility of the Principal:

I. To take overall responsibility for e-safety provision

II. To take overall responsibility for data and security (SIRO)

III. To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements

IV. Co-ordinate action within the school in cases of suspected e-safety issues and to liaise with the appropriate agencies.

V. To receive regular monitoring reports from the E-safety co-ordinator

VI. Facilitate in-service training or awareness and recognition of E-safety issues.

VII. Establish clear procedures and lines of communication so that all staff know what to do in the event of misuse of technology by any member of the school community and know how to act if they have concerns or need support regarding E-safety issues.

VIII. Keep present and new staff informed about E-safety issues

IX. Check the IT system for any misuse

X. Keep a written record of any E-safety concerns and manage any E-safety incidents by following the flow chart for managing E-safety incidents in Appendix

XI. To ensure there is a system in place to monitor and support staff who carry out internal e-safety procedures

E-Safety Co-ordinator

4.2 It is the role and responsibility of the E-safety Co-ordinator:

I. To take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies/ documents

II. Provide resources and materials for E-safety e.g.:

Posters

PSHCE

III. To promote an awareness of and commitment to e-safeguarding throughout the school community

IV. To ensure that e-safety is embedded across the curriculum

V. To liaise with IT technical staff

VI. To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering/ change control logs

VII. To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident

VIII. To ensure that an e-safety incident log is kept up to date

IX. To facilitate training and advice for all staff, including new staff and those on university/ college placement

X. To liaise with relevant agencies

XI. To keep regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/ inappropriate materials
- Inappropriate on-line contact with adults/ strangers
- Potential or actual incidents of grooming
- Cyber-bullying and use of social media

Governors/ E-safety Governor

4.3 It is the role and responsibility of the school governors:

I. To ensure that the school follows all current e-safety advice to keep the children and staff safe

II. To approve the E-safety policy and review the effectiveness of the policy. A member of the Governing Body will take on the role of E-safety Governor.

III. To support the school in encouraging parents and the wider community to become engaged in e-safety activities

IV. The E-safety governor will review e-safety incidents with the E-safety co-ordinator.

Computing Co-ordinator

4.4 It is the role and responsibility of the Computing co-ordinator:

I. To oversee the delivery of the e-safety element of the Computing curriculum

II. To liaise with the e-safety co-ordinator regularly

The Staff

4.5 It is the role and responsibility of the staff:

I. To read, understand and help promote the school's e-safety policies and guidance

II. To read, understand, sign and adhere to the school staff Acceptable Usage Agreement/ Policy

III. To embed e-safety issues in all aspects of the curriculum and other school activities

IV. To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant)

V. To ensure that pupils are fully aware of research skills and are aware of legal issues relating to electronic content such as copyright laws

VI. To be aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices

VII. To report any e-safety related issues that arise to the E-safety Co-ordinator

VIII. Report any misuse of technology to the Principal or E-Safety Co-ordinator

IX. To maintain an awareness of current e-safety issues and guidance e.g. through CPD

X. To model safe, responsible and professional behaviours in their own use of technology

XII. To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. mail, text, mobile phones etc.

XIII. Provide opportunities that enable children to take and make decisions for themselves

XIV. Help children to develop an awareness of the sources of danger and the strategies for avoidance and problem solving.

XV. Create a school/classroom atmosphere where children feel secure, are listened to and valued.

The Pupils

4.6 It is the responsibility of the pupils:

I. To read, understand, sign and adhere to the Pupils Acceptable Usage Policy (At Key Stage 1 it would be expected that parents/ carers would sign on behalf of their child)

II. To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

III. To understand the importance of reporting abuse, misuse or access to inappropriate materials

IV. To know what action to take if they, or someone they know, feels worried or vulnerable when using online technology

V. To know and understand school policy on the use of mobile phones, digital cameras and hand held devices

VI. To know and understand school policy on the taking/ use of images and on cyber-bullying

VII. To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school (e.g. the school blog)

VIII. To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home

IX. To help the school in the creation/ review of e-safety policies (through review with the school council)

Parents/ Carers

4.7 It is the responsibility of parents/ carers:

I. To support the school in promoting e-safety and endorse the Parent's Acceptable Usage Agreement which includes the pupil's use of the internet and the school's use of photographic and video images

II. To read, understand and promote the school Pupil Acceptable Usage Agreement with their children

III. To access the school website/ learning platform/ blog/ social media pages in accordance with the relevant school Acceptable Usage Agreement

IV. To consult with the school if they have any concerns about their children's use of technology

5 E-Safety in the Curriculum

5.1 IT and online resources are increasingly used across the curriculum. E-safety guidance shall be given to the pupils on a regular and meaningful basis. E- Safety shall be embedded within the curriculum.

5.2 Internet use shall be carefully planned to ensure it is age-appropriate and supports the learning objectives for specific curriculum areas.

5.3 Opportunities within a range of curriculum areas will be utilised to teach about E-safety.

5.4 Pupils will be educated about the dangers when using technologies outside school. (This shall be done informally when opportunities arise and as part of the E safety curriculum).

5.5 Pupils shall be made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do, but also serves to protect them.

5.6 Pupils shall be taught about copyright and respecting other people's information, images etc. through discussion, modelling and activities.

5.7 Pupils will be reminded about their responsibilities through the use of an acceptable use of computers and the internet agreement which will be signed by the pupil and parent/ carer and will be displayed in school.

5.8 Staff will model responsible and safe behaviour in their own use of technology during lessons.

5.9 E-Safety shall be promoted throughout the school through the use of a clear and progressive e-safety education programme, as part of the Computing curriculum. This includes teaching children:

I. To stop and think before they click

II. To develop a range of strategies to evaluate and verify information before accepting it's accuracy

III. To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be

IV. to know how to narrow down or refine a search

V. [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings

VI. to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private

VII. to understand how photographs can be manipulated and how web content can attract the wrong sort of attention

VIII. to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments

IX. to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings

X. to understand why they must not post pITures or videos of others without their permission

XI. to know not to download any files – such as music files - without permission

XII. to understand the issues around aspects of the commercial use of the internet as age appropriate. This may include risks in pop-ups, buying on-line and on-line gaming

XIII. to have strategies for dealing with receipt of inappropriate materials

XIV. [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons

XV. To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying

XVI. To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

6 Password Security

6.1 Staff shall keep passwords secure and must not share them with anyone.

6.2 All users shall read and sign an “Acceptable Use Agreement” to demonstrate that they have understood the school’s E-safety policy

6.3 Users shall be provided with a log-in username and shall use a personal password which they must keep private

6.4 Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

6.5 If a user of the system thinks their password may have been compromised or someone or someone else has become aware of the password it must be reported to IT Support who will immediately change the password.

6.6 Staff shall be made aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared.

6.7 Individual staff users must ensure that work stations are not left unattended and are locked.

.

7 Data Security

7.1 The accessing and appropriate use of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008)

7.2 The level of access shall be determined by the Principal

7.3 Staff shall be aware of their responsibility when accessing school data.

7.4 Staff shall be made aware of how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection

7.5 Any data taken off the school premises must be encrypted.

7.6 Data can only be accessed and used on school computers or laptops. Staff must not use their personal devices for accessing any school/ children/ pupil data.

8 Managing the Internet

8.1 All use of the Northern Grid for Learning (NGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

8.2 The school will provide pupils with supervised access to internet resources through the school's fixed and mobile internet technology.

8.3 Staff will preview any recommended sites before use.

8.4 Raw image searches are discouraged when working with pupils.

8.5 If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

8.6 All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

8.7 All users must observe copyright of materials from electronic resources.

Infrastructure

8.8 Kader School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

8.9 There is a monitoring solution via the Northern Grid for Learning where web-based activity is monitored and recorded.

8.10 School internet access is controlled through the web filtering service "Threat Management Gateway" (TMG)

8.11 The school also employs some additional web filtering (IMPERO) which is the responsibility of the Systems Manager. IMPERO provides detailed logs and real time monitoring.

8.12 The school is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

8.13 School based email and internet activity can be monitored and explored further if required.

8.14 The school does not allow pupils access to internet logs.

8.15 The Principal has responsibility of randomly checking staff internet logs

8.16 The school uses management control tools for controlling and monitoring workstations.

8.17 If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the E-safety co-ordinator.

8.18 It is the responsibility of the school, by delegation to the Systems Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

8.19 Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility or the network manager's responsibility to install or maintain virus protection on personal systems. If pupils wish to bring work on removable media it must be given to the School office for a safety check first.

8.20 If there are any issues related to viruses or anti-virus software, the IT Systems Manager must be informed

9 Managing Social Media

Social Media is the popular term for advanced Internet technology and applications including blogs, wikis, RSS and social networking including sites such as Instagram, Facebook and Twitter. The school endeavours to protect and educate staff and pupils in the use of social media, including what measures are in place to intervene and support should an issue arise.

9.1 The school endeavours to deny access to social networking sites to pupils and staff for personal use within working sessions.

9.2 All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

9.3 Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

9.4 Pupils are always reminded to avoid giving out personal details (e.g. full name, address, mobile/ home phone numbers, school details, IM / email address, specific hobbies/ interests) on sites which may identify them or their location.

9.5 Pupils are asked to report any incidents of on-line bullying to the school.

School staff should ensure that:

9.6 No reference should be made in social media to students, parents/ carers or school staff.

9.7 They do not engage in online discussion on personal matters relating to members of the school community.

9.8 Personal opinions should not be attributed to the Academy.

9.9 Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The Academy's use of social media for professional purposes will be managed and closely monitored by the Principal and e-safety committee to ensure compliance with the relevant policies.

10 Mobile Technologies

10.1 At Kader Academy the use of these devices is managed in the following ways so that they are used appropriately.

Personal Mobile devices (including phones)

10.2 The school allows staff to bring in personal mobile phones and other personal devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

10.3 Staff mobile phones should only be used in the staff room and office area.

10.4 In case of an emergency friends and relatives should contact the school via the landline.

10.5 Pupils are not allowed to bring personal mobile devices and/ or phones to school.

10.6 The school is not responsible for the loss, damage or theft of any personal mobile device.

10.7 The sending of inappropriate text messages between any members of the school community is not allowed.

10.8 Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

10.9 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices

10.10 Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

10.11 Where the school provides mobile technologies such as phones, i-pads and laptops for offsite visits and trips, only these devices should be used.

10.12 Where the school provides a laptop or i-pad for staff, this device may only be used to conduct school business outside of school and for ‘reasonable personal use’

11 Managing Email

11.1 The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private.

11.2 All staff have their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

11.3 It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all email is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.

11.4 Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

11.5 Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.

11.6 Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

11.7 Y1 to Y6 pupils have their own individual school issued accounts

11.8 The forwarding of chain letters is not permitted in school.

11.9 All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments.

11.10 Pupils must immediately tell a teacher / trusted adult if they receive an offensive email.

11.11 Staff must inform (the E-safety Leader / line manager) if they receive an offensive email.

11.12 Pupils are introduced to email as part of the Computing Scheme of Work.

11.13 Incoming and outgoing emails into the school email system which contain inappropriate language or content will be picked up through the filtering system. Any violation of this kind will be reported directly to the E-safety officer by the Systems Manager and appropriate action taken.

11.14 The school reserves the right to monitor all email activity.

12 Safe Use of Images

12.1 Digital images are easy to capture, reproduce and publish. It is not appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

12.2 With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

12.3 Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

12.4 Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

Publishing pupil's images

12.5 On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's photographs in the following ways:

I. on the school web site and related professional social media accounts

II. on the school's Learning Platform

III. in the school prospectus and other printed publications that the school may produce for promotional purposes

IV. recorded/ transmitted on a video/DVD or webcam

V. in display material that may be used in the school's communal areas

VI. in display material that may be used in external areas, i.e. exhibition promoting the school

VII. general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

12.6 This consent form is considered valid for the entire period that the child attends Kader Academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

12.7 Parents / carers may withdraw their permission, in writing, at any time.

12.8 Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

12.9 Only the School secretary has permission to upload content to the site once authorisation has been given by the Principal.

Storage of Images

12.10 Images / films of children may be stored on the school's network

12.11 Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB memory sticks) without the express permission of the Principal

12.12 Rights of access to images are restricted to the teaching staff and pupils within the confines of the school network / Learning Platform.

12.13 The Systems Manager has the responsibility of deleting images when they are no longer required, or the pupil has left the school.

Video Conferencing

12.14 All pupils shall be supervised by a member of staff when video conferencing.

12.15 All pupils shall be supervised by a member of staff when video conferencing with end-points beyond the school.

12.16 The school shall keep a record of video conferences, including date, time and participants.

13 Misuse and Infringement

Complaints

13.1 Complaints relating to e-safety should be made to the E-safety Leader or Principal. Incidents should be logged and the Flowcharts for Managing an e-safety incident should be followed (see Appendix).

Inappropriate material

13.2 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-safety co-ordinator.

13.3 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety Leader followed by investigation. Depending on the seriousness of the offence the individual may be subject to immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

14 Pupils with Additional Needs

14.1 The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules.

14.2 Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their knowledge and understanding of e-safety issues.

14.3 Where a pupil has poor social understanding, careful consideration shall be given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

15 Parental Involvement

15.1 It is important for parents / carers to be fully involved with promoting E-safety both in and outside of school. The school shall seek to promote a wide understanding of the benefits related to IT and associated risks.

15.2 Parents / carers will be asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

15.3 Parents / carers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g. on the school website)

15.4 The school will run a rolling programme of advice, guidance and support for parents, including:

I. The introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear

II. Information leaflets; information in school newsletters and on the school website

III. Demonstrations and parent information sessions

IV. Suggestions for safe internet use at home

V. Provision of information about national support sites for parents.

16 Reviewing the Policy

16.1 There will be an on-going opportunity for staff to discuss with the Principal and E-safety Leader any issue of E-safety that concerns them.

16.2 This policy will be reviewed annually and consideration given to the implications for future whole school development planning.

16.3 The policy will be amended if new technologies are adopted or Central Government changes any legislation.

17 APPENDICES

17.1 Flowchart for Managing E-Safety Incidents

17.2 Incident Log

17.3 Current Legislation

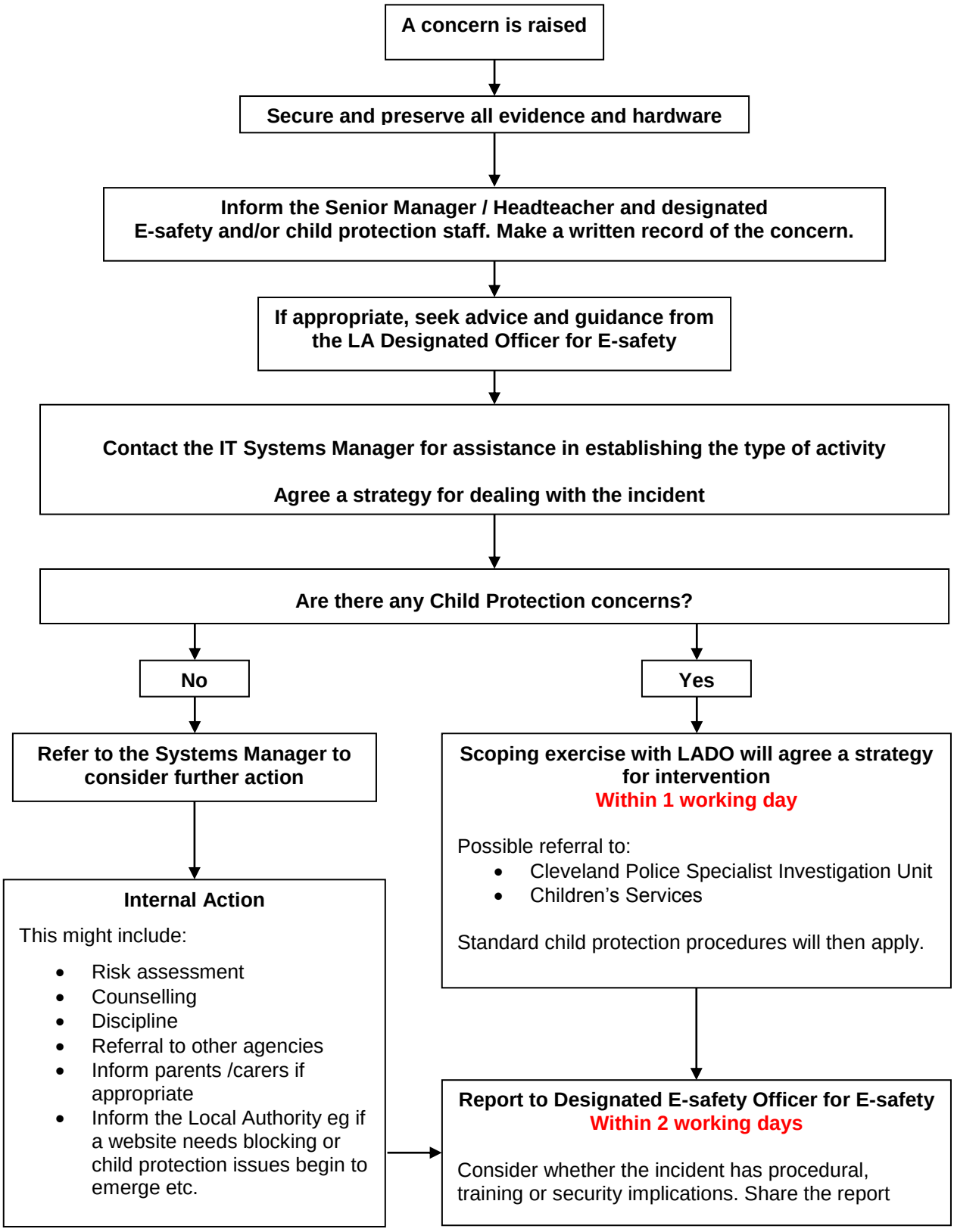
17.4 Acceptable Use Agreement & Code of Conduct for Staff, Governors and Visitors

17.5 KS1 Pupil Agreement: Policy for Acceptable Use of Computers & the Internet

17.6 KS2 Pupil Agreement: Policy for Acceptable Use of Computers & the Internet

17.7 Letter to Parents: Photographs, Video or Film Consent Form

Flowchart for Managing E-Safety Incidents



E-safety Incident Log

Date & Time	Name of Pupil and/or Staff Member	Room and computer/device number	Details of incident (including evidence)	Actions & reasons

Current Legislation

Acts relating to monitoring of staff email

- Data Protection Act 1998
- The Telecommunications (Lawful Business Practice)
- (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998

Other Acts relating to E-safety

- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- The Computer Misuse Act 1990 (sections 1 – 3)
- Malicious Communications Act 1988 (section 1)
- Copyright, Design and Patents Act 1988
- Public Order Act 1986 (sections 17 – 29)
- Protection of Children Act 1978 (Section 1)
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 199

Acceptable Use Policy: Staff, Governors and Visitors

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This policy is designed to ensure:

- that all staff are aware of their professional responsibilities when using any form of IT;
- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school / academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement/ Code of Conduct

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, i-pads, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Governing Body.
- I will not install any hardware of software without permission of E Learning Co-ordinator.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the

Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I understand that this Acceptable Use Policy applies not only to my work and use of academy ICT equipment in school, but also applies to my use of academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include, in the event of illegal activities, the involvement of the police.

Any concerns or clarification should be discussed with the Principal or a member of the e-safety committee. I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Full Name **(Print)**

Job Title **(Print)**

Signature **Date:**

Kader Academy

Staindrop Drive, Acklam, Middlesbrough, TS5 8NU

Tel: 01642 286599, Fax 01642 286599

Principal: Mrs L Chalk

Acceptable Use of Computers and the Internet Agreement for Early Years and Key Stage 1 Pupils

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

School's Responsibilities

This Acceptable Use Policy is designed to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Signed by
Principal: _____ Print Name: _____

Kader Academy

Staindrop Drive, Acklam, Middlesbrough, TS5 8NU

Tel: 01642 286599, Fax 01642 286599

Principal: Mrs L Chalk

Children's Responsibilities

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will only click on icons and links after I have checked with a teacher or suitable adult so I know they are safe.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on a screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed by pupil: _____ Print Name: _____

Parents' Responsibilities

Please read the agreement below and sign to say that you agree.

- I give permission for my son/ daughter to have access to the internet and to ICT systems at school.
- I understand that the school has discussed the Acceptable Use Agreement with my son/ daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed by
Parent/Carer: _____ Print Name: _____

Kader Academy

Staindrop Drive, Acklam, Middlesbrough, TS5 8NU

Tel: 01642 286599, Fax 01642 286599

Principal: Mrs L Chalk

Acceptable Use of Computers and the Internet Agreement for Key Stage 2 Pupils

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

School's Responsibilities

This Acceptable Use Policy is designed to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Signed by
Principal: _____ Print Name: _____

Parents' Responsibilities

Please read the agreement below and sign to say that you agree.

- I give permission for my son/ daughter to have access to the internet and to ICT systems at school.
- I know that my son/ daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the

importance of safe use of technology and the internet – both in and out of school.

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed by Parent/Carer: _____ Print Name: _____

Kader Academy

Staindrop Drive, Acklam, Middlesbrough, TS5 8NU

Tel: 01642 286599, Fax 01642 286599

Principal: Mrs L Chalk

Acceptable Use Policy Agreement – Key Stage 2 Pupils

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school / academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school / academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school / academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

Kader Academy

Staindrop Drive, Acklam, Middlesbrough, TS5 8NU

Tel: 01642 286599, Fax 01642 286599

Principal: Mrs L Chalk

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

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

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

Signed by pupil: _____ Print Name: _____

Date: _____

Kader Academy

Staindrop Drive, Acklam, Middlesbrough, TS5 8NU

Tel: 01642 286599, Fax 01642 286599

Principal: Mrs L Chalk

Use of Digital/ Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. On occasion the media is invited into the academy to take photographs, film footage or video recordings which would then be available to the wider community.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

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

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

With reference to the above, please complete the form below and return it to school.

Yours sincerely,

Mrs. L. Chalk,
Principal.

Digital/ Video Images Permission Form

Child's Name: _____ **Class:** _____

Parent/ Carers Name: _____

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed _____

Date _____