E-Safety

Policy

Revised February 2017

Background/Rationale

New technologies have become integral to the lives of young people in today's society, both within schools and in their lives outside school. The development and expansion of the use of Computing, and particularly of the internet, has transformed learning in recent years. Pupils need to develop high level computing skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that computing can bring to teaching and learning.

The purpose of this e-Safety policy is to ensure that Knowle CE Primary Academy meets its statutory obligations and that pupils are safe and protected from potential harm, both within and outside school.

The requirement to ensure that pupils are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care, to which all who work in Knowle CE Primary Academy are bound. The academy e-Safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyber bullying;
- Access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the student.

Scope of the Policy

This policy applies to all the members of the Knowle CE Primary Academy community (including staff, governors, pupils, parents/carers and visitors,) who have access to and are users of academy ICT systems, both in and out of the academy.

Role and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school.

The Principal and Governors have ultimate responsibility to ensure that the E-Safety Policy is monitored in conjunction with the Computing and PSHE Leads.

The senior management team and Governors are kept informed by subject leaders. All Governors have an understanding of the issues and that strategies at Knowle CE Primary Academy are in relation to local and national guidelines and advice.

Principal and senior leaders

- The Principal is responsible for ensuring the safety (including E-Safety) of members of the academy.
- The Principal and Senior Leaders are responsible for ensuring that all relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.

Teaching, Support Staff and Extended Services

Are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices;
- they have read, understood and signed the schools Staff, Governors and Visitors Acceptable Use Policy (See appendix 1)
- they report any suspected misuse or problem to a member of the Senior Leadership Team or Computing Lead
- digital communications with pupils (email/ online program e.g. Purple Mash) should be on a professional level and only carried out using official school systems;
- E-Safety issues are embedded in all aspects of the curriculum and other school activities;
- pupils understand and follow the school e-Safety and acceptable use agreement
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor computing activity in lessons, extra-curricular and extended school activities;
- they are aware of E-Safety issues related to the use of mobile phones, cameras, iPads and other hand held devices and that they monitor their use and implement current school policies with regard to these devices. See Mobile Devices Policy (Appendix 2)
- in lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead (DSL):

Will be trained in E-Safety issues 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;
- cyberbullying.

Pupils

- are responsible for using the school computing systems in accordance with the Pupils Rules For Responsible Internet Use Agreement (see appendix 3) which they and/or their parents/carers will be expected to sign before being given access to school systems;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand school policies on the use of mobile phones, digital cameras, iPads and other mobile devices. They should also know and understand school policies on the taking/use of images and on cyber bullying;
- should 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.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of Computing than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, the school website, e-safety meetings for parents and information about national/local e-safety campaigns/literature.

Parents and carers will be responsible for:

- discussing the Pupil Rules For Responsible Internet Use Agreement with their child and endorse it (by signature).
- promote the school values and rules for responsible internet use when their child accesses the internet outside of school.

Teaching and Learning

Why is it important?

The internet is an essential element in 21st century life for education, business and social interaction. It is an open communications channel allowing information to be transmitted to many locations in the world. Messages may be sent, ideas discussed and material published, with very little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

The purpose of Internet use in school is to increase pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration systems.

The statutory curriculum requires pupils to learn how to create, organise, store, manipulate and retrieve digital content. In addition they need to identify where to go for help and support when they have concerns about content or contact on the internet. Also pupils need to search technologies effectively. Consequently, in delivering the computing curriculum, teachers need to use the 'Progression in Computing Document' to integrate the use of communications technology such as web-based resources and e-mail to enrich and extend learning activities.

How Internet enhances learning

- The school Internet access will be designed expressly for pupil use and includes filtering content so that it is appropriate to the age of pupils.
- Pupils will be taught about acceptable Internet use and given clear objectives for Internet use.
- Pupils will be educated in the effective use of Internet research, including the skills of knowledge location, retrieval and evaluation.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Pupils taught how to evaluate internet content.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- E-Safety is embedded across all aspects of the computing curriculum, as evidenced in the progression document, and delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools.

Core Principles of Internet Safety

In common with most technologies, Internet use presents risks as well as benefits. Pupils could be placed in inappropriate and even dangerous situations without mediated Internet access. To ensure responsible use and the safety of pupils the school's policy is based upon five core principles:

Guided educational use

Internet use will be planned, task orientated and educational within a regulated and managed environment.

Risk assessment

Both staff and pupils will be aware of the risks associated with Internet use.

Emerging technologies will be examined for educational benefit before use in school is allowed. Staff and pupils will know what to do if they come across inappropriate material when using the Internet.

Responsibility

Internet safety depends on staff, governors, parents, and, where appropriate, pupils themselves taking responsibility for use of the Internet and associated technologies. The school will seek to balance education for responsible use, regulation and technical solutions to ensure pupils' safety.

Regulation

The use of the Internet, which brings with it the possibility of misuse, will be regulated. Fair rules, written for pupils to read and understand, are prominently displayed as a constant reminder of the expectations regarding Internet use.

Appropriate Strategies

Effective, monitored strategies are in place to ensure responsible and safe Internet use. The school will work in partnership with the LA, DFE, parents and the Internet Service Provider to ensure systems which protect pupils are regularly reviewed and improved.

Managing Information Systems

Information System Security

Computing security is a complex issue.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The system capacity will be reviewed regularly.
- Use of user logins and passwords to access the school network will be enforced

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone, without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised by the class teacher, before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Passwords

The academy will be responsible for ensuring that the academy infrastructure and network is as safe and secure as is reasonably possible. Therefore a safe and secure username/password system will apply to all academy computing systems, including email. In addition;

- users can only access data to which they have right of access;
- no user will be able to access another's files, without permission (or as allowed for monitoring purposes within the academy's policies);
- access to personal data will be securely controlled in line with the academy's personal data policy.

All users will have responsibility for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Members of staff will be made aware of the school's password security procedures:

- at induction;
- through the school's e-Safety policy;
- through the Acceptable Use Agreement;

Students will be made aware of the school's password security procedures:

- in computing lessons
- through the Acceptable Use Agreement

The Senior Leadership Team and Computing lead should have a centrally located record of:

- User Ids and requests for password changes;
- User log-ons;
- Security incidents related to this policy.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. User lists, IDs and other security related information will be given the highest security classification and stored in a secure manner.

Managing Email

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; for example, projects between pupils, schools – both locally and nationally and as part of the global community.
In the Academy context, email is not considered private and Knowle CE Primary Academy reserves the right to monitor academy email. However, there is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with staff, parents/carers, pupils and other professionals for any official academy business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Spam, phishing and virus attachments can make email dangerous. The school ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily.

E-mailing confidential data is not recommended and should be avoided where possible. Where the conclusion is that e-mail must be used to transmit such data it is essential that staff:

- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail
- Verify the details, including accurate e-mail address, of any intended recipient of the information;
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information;
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
- Send the information as an encrypted document **attached** to an e-mail;
- Provide the encryption key or password by a **separate** contact with the recipient(s);
- Do not identify such information in the subject line of any e-mail;
- Request confirmation of safe receipt.

Published content on the school website

- The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The School Business Manager and Principal will take overall editorial responsibility and ensure that content is accurate and appropriate. The computing lead will support in ensuring this information is accurately provided on the schools website.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, pupils and parents/carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should

recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images. Pupils should be appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, in particularly in association with photographs.
- Written permission from parents or carers will be obtained during September of each academic year before photographs of pupils are published on the schools website. (Permission for Academy Activities Form)
- Pupils work can only be published with the permission of the pupil and parents or carers.

Managing Social Networking, Social Media and Personal Publishing Sites

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

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

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others. Please refer to the Social Media Policy for further details (See Appendix 4)

Managing Filtering

- The school will work in partnership with Solihull MBC to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Solihull ICT Services and where appropriate the Computing lead and the Senior Leadership team.

Managing Videoconferencing

Videoconferencing, including Skype, enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer**.**
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- Equipment must be secure and locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission of the Principal.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Users:

- Pupils will not be allowed to make videoconference calls without the supervision of an adult in a planned computing lesson.
- Videoconferencing will be supervised and appropriately targeted for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences through the 'Permission Form For Academy Activities' form.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.

Content:

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, it is important to check that they are delivering material that is appropriate for your class.

<u>Webcams</u>

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, and never used to take images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions.
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit before use in school is allowed.
- Mobile phones are not allowed to be used during contact time and must be placed in a secured area. The sending of abusive or inappropriate text messages is forbidden.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.

Data Protection

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

Appendices

Appendix 1 – Staff, Governors and Visitors Acceptable Use Agreement

Appendix 2 – Mobile Devices Policy

Appendix 3 – Pupils Rules For Responsible Internet Use

Appendix 4 – Social Media Policy

Appendix 1 – Staff, Governors and Visitors Acceptable Use Agreement

Acceptable Use Agreement – Staff, Governors and Visitors

I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - pornography (including child pornography)
  - promoting discrimination of any kind
  - promoting racial or religious hatred
  - promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes children in my care to danger
- distribute any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law
- use the internet for non-work related purposes during contact time with pupils.

I accept that my use of the Academy and Local Authority Computing facilities may be monitored and the outcomes of the monitoring may be used.

I have read and acknowledged the Academy's Social Media and Mobile Devices polices.

I have read, understood and agree with the Acceptable Use Agreement.

Signed:…… Print Name …….. Date:…….

Appendix 2 – Mobile Devices Policy

Knowle CE Primary Academy

Mobile Device Policy

Knowle CE Primary Academy is committed to ensuring the safety of children in its care. We recognise the importance of mobile devices in school for communication purposes, but are aware that casual or inappropriate use of mobile devices in the Academy could pose a risk to children.

This policy applies to all individuals who have access to personal or work-related devices on site. It does not apply to educational* mobile devices. This includes staff, volunteers, pupils, governors, parents, carers, visitors and community users. This list is not exhaustive.

Introduction

Mobile technology has advanced significantly over the last few years - and it continues to evolve. Wireless connections in particular have extended the capabilities of mobile devices, enabling access to a wide range of new content and services globally. Many phones now offer Internet and email access, alongside the often standard functions of messaging, camera, video and sound recording. Mobile phones, alongside other forms of technology are changing the way and speed in which we communicate. They can provide security and reassurance; however there are also associated risks.

Children and young people need to understand these risks in order to help them develop appropriate strategies for keeping themselves safe. As with e-safety issues generally, risks to children and young people can be broadly categorised under the headings of content, contact and conduct and managed by reducing availability, restricting access and increasing vigilance.

Aim

The aim of the Mobile Devices Policy is to promote safe and appropriate practice through establishing clear and robust acceptable use guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile devices are effective communication tools - which in turn can contribute to safeguarding practice and protection.

Policy statement

It is recognised that it is the enhanced functions of many mobile devices that cause the most concern, and which are most susceptible to misuse. Misuse includes the taking and distribution of indecent images, exploitation and bullying.

When mobiles devices are misused it can impact on an individual's dignity, privacy, right to confidentiality and safety. Such concerns are not exclusive to pupils and hence there is a duty to protect the needs and vulnerabilities of all.

** iPads, laptops, netbooks, 'Go Pro' video camera, digital cameras which are owned by Knowle CE Primary Academy and licenced specifically for school use.*

It is appreciated that it can be very difficult to detect when such devices are present or being used, particularly in relation to enhanced functions, such as cameras. The use of all mobile devices is therefore limited, regardless of their capabilities. The aim is to avoid distraction and disruption of the working day, and to minimise the opportunities for any individual to make any covert images or misuse functions in any other way. Therefore Knowle CE Primary Academy limits the use of **personal** mobile devices for any purpose to specific areas of the building.

These are:

- Outside the main reception office doors
- Inside the Principal's office
- Inside the school staff room

In all other areas personal mobile devices should be turned off or be on silent and stored away from view. Personal mobile phones should not routinely be carried on an individual's person except to transport it to or from the designated area eg from a classroom to the staffroom at lunchtime.

A zero-tolerance policy is in place with regards to the use of personal mobile phones by any individual outside of these areas.

Code of Conduct

Staff

There is an expectation that all personal use of mobile devices is limited to allocated lunch and/or breaks and only in the designated areas (see above).

Staff will not carry personal mobile devices during working hours. In this instance 'working hours' is deemed to be 'directed time' which, in most cases, corresponds to the period of time when children are receiving education or childcare provision. This protects staff from being distracted from their work and from possible allegations of inappropriate use but ensures that staff who are working on-site outside of 'directed time' are contactable in the event of an emergency.

Staff must give the Academy telephone number to their next of kin in case it is necessary for the staff member to be contacted in an emergency during the school day.

Under no circumstances is any member of staff permitted to take images of pupils or make recordings on their personal mobile devices. School cameras/iPads are available for this purpose.

Any member of staff bringing a personal device into the Academy must ensure that it contains no inappropriate or illegal content.

It is also advised that staff 'security protect' access to their mobile devices.

If a member of staff needs to make telephone contact with a parent, a school phone should be used.

All staff must remain vigilant at all times and there is an expectation that they will challenge any misuse of a mobile device on the Academy site.

Any breach of this policy may result in disciplinary action being taken.

Exceptional Circumstances

Knowle CE Primary Academy is an extended site and there are a number of business mobile phones allocated to designated members of staff. These are:

- Caretaker's Phone
- Extended Services' mobile phones (x2)
- Breakfast Buddies' mobile phone
- Principal's mobile phone
- Business and Facilities Manager's phone

These have been allocated to staff to aid effective communication; provide an essential part of emergency procedures; enable out of hours contact and provide a backup facility should problems be experienced with the land line. It is expected that where possible these phones are used out of the vicinity of children.

Under no circumstance must the Academy business mobile phones be used to take photographs or videos of pupils in the school. Personal calls are not permitted to be made on any work mobile other than in agreed exceptional circumstances. All calls made on work mobile phones may be logged.

Educational Visits

Mobile phones are needed for communication purposes by staff/group leaders to stay in contact with each other during the visit. The leader of each group may carry and use a personal mobile phone for this purpose only. Under no circumstances should the phone be used to take images of any children. A school camera is available should staff wish to take photos during the visit.

The use of mobile phones on education visits will be incorporated into individual Risk Assessments.

Year 6 Residential

Pupils are not allowed to take any mobile devices on the Year 6 residential visit. However, they are allowed to take their own personal camera. Year 6 parents will be asked to complete a permission form with regard to their child being included on another child's photographs. In the event that this permission is not given staff will ensure that parent's wishes are observed.

Parents/Carers/Visitors

Parents/carers and visitors to Knowle CE Primary Academy are asked to turn off their mobile devices on entry to the main office and are instructed not to use their devices in the school buildings. Parents should be aware that they will be challenged if they are observed breaching this policy. Signs are displayed around the school as a reminder.

Taking Photographs at Celebration Events/Performances

When parents/carers have been invited to attend a 'celebration' event the member(s) of staff in charge of the event will instruct Parents/Carers that mobile devices may be used as ***cameras only*** at a specific point during the event eg at the end of the performance. This will ensure that the Academy is able to discharge its statutory responsibility to safeguard pupils. Parents and carers must only take a photograph of their own child, taking care to ensure that no other child is included in the photograph without the express permission of that child's parents.

It is recognised that many parents and carers wish to have a visual record of special events which take place in school. To accommodate this Knowle CE Primary Academy will organise an official DVD recording of the key events which parents may purchase eg Nursery Nativity, Year 2 Summer Entertainment, and Year 6 Leavers Presentation Evening. These recordings will have been subjected to the necessary safeguarding protocols.

We must insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own.

Annual Sports Days/Competitive Team Events

Sports Days are an annual event involving all the pupils in the school at which we allow photographs to be taken at any point during the event. We would ask that parents who take photos of their child taking part are mindful of the need to avoid including other children in their photographs. **We must insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own**.

Parents of pupils who represent the school in competitive sports events eg Borough Sports/Athletics will be asked to give their permission for team photographs to be taken by other parents at the event.

Children bringing Mobile Phones into School

Knowle CE Primary Academy discourages pupils from bringing mobile phones to school on the grounds that they may be lost, stolen or misused. However, we appreciate that older children in Years 5 & 6 may walk to and from school independently and parents may wish their child to have a phone. If this is the case permission must be granted by the Principal. A form is available for this purpose from the school office. All children's phones must be switched off and handed in to the Class Teacher on arrival where they will be stored until the end of the school day.

Should a pupil be found to be using a phone inappropriately, the Academy reserves the right to withdraw this privilege and they may no longer be able to bring a phone into school.

Contractors/Agencies/Catering Staff

These will be subject to this policy; any exceptions will need to be agreed with the Principal in advance.

Knowle CE Primary Academy

Kixley Lane, Knowle, Solihull B93 0JE

Tel: 01564 776209
www.knowle.solihull.sch.uk
Email: office@knowle.solihull.sch.uk

Principal: Miss J Godsall
Vice Principals: Mrs E Clarke, Mr M Stonehill
Business and Facilities Manager: Mrs E Lynch

20 September 2016

Dear Parent/Carer

Re: Mobile Phone Permission

If you require your child to have a mobile phone in school because they walk home independently please complete and return the slip below noting the following:

- Your child needs to hand the phone into their class teacher on arrival in the morning.
- All phones should be appropriately named for identification purposes
- Knowle CE Primary Academy bears no responsibility for any loss or damage to the mobile phone
- Should your child be found to be using their mobile phone inappropriately we reserve the right to withdraw this privilege

Yours sincerely

Jenny Godsall

Jenny Godsall
Principal

✂……

To: Miss Godsall, Knowle CE Primary Academy

Name of Child…… Class ……

My child needs to bring their mobile phone into school as they regularly walk to or from school independently.

Signed ……Parent/Guardian Date……

Approved by:

……Jenny Godsall, Principal Date……

Appendix 3 – Pupils Rules For Responsible Internet Use

Rules for Responsible Internet Use

When I am using the computer or other technologies, I want to feel safe all the time

I AGREE THAT I WILL

- Always keep my passwords a secret
- Only visit sites which are appropriate to my work at the time
- Work in collaboration only with friends and I will deny access to others
- Tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- Make sure all messages I send are respectful
- Show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- Not give my mobile phone number to anyone who is not a friend
- Only e-mail people I know or those approved by a responsible adult
- Only use e-mail which has been provided by school
- Talk to a responsible adult before joining networking sites
- Always keep my personal details private (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- Always check with a responsible adult and my parents before I show photographs of myself or anyone else
- Never meet an online friend without taking a responsible adult that I know along with me
- I know that once I post a message or an item on the internet then it is completely out of my control
- I know that anything I write or say or any website that I visit may be being viewed by a responsible adult

Pupil Agreement:

I have read and understand the Pupil Rules for Responsible Use of the Solgrid Internet. I will follow these rules at all times

Signed: …… Date: …….

Full Name: …… Class: ……

Appendix 4 – Social Media Policy

Social media policy

For school staff

Created: June 2015

Contents

1	Introduction	3
2	Objectives	3
3	Responsibility and accountability	4
4	When using social media at any time	5
5	When using social media on behalf of the school	6
6	When using social media as part of working with pupils and students	7
7	When using social media in staff's wider professional life	7
8	When using social media in staff's personal life	7
9	Excessive use of social media at school	9
10	Monitoring use of social media on school equipment	9
11	Disciplinary action over social media use	9
12	If you have any concerns	9

1 Introduction

1.1 We actively encourage the responsible use of social media. Responsible use of social media can be positive for learning and teaching. It can also be personally enjoyable and beneficial.

1.2 This policy will make clear what standards are expected of anyone who works for the school and uses social media as well as what actions may be taken when it is considered a member of staff may have breached this policy.

1.3 This policy applies to all staff use of social media, including:

1.3.1 on behalf of the school;

1.3.2 as part of their work directly with pupils ;

1.3.3 in their wider professional lives; and

1.3.4 in their personal lives.

1.4 There is additional guidance available to help staff follow good practice on the e-safety toolkit area of the Social Solihull website.

1.5 In this policy, we define social media to mean:

'Websites and applications that enable users to create and share content or to participate in social networking.'

1.6 In this policy, the word staff includes temporary and casual staff, agency staff, and volunteers during their time working with the school.

1.7 In this policy, the word parents is used to mean the parents, carers and others with parental responsibility for a pupil at the school.

1.8 This policy works alongside other legislation, DFE statutory guidance, and other school and local authority policies such as Code of employee conduct, E safety framework policy and Acceptable use agreement. These all also apply where relevant.

2 Objectives

The purpose of this policy is to;

(a) clarify what the school considers to be appropriate and inappropriate use of social networking by staff;

(b) encourage social networking to be used in a beneficial and positive way;

(c) safeguard staff, pupils, parents and members of the public from abuse through social networking;

(d) safeguard the reputation of the school, other schools, other organisations and employers from unwarranted abuse through social networking; and

(e) set out the procedures that will be followed where it is considered that staff have inappropriately or unlawfully used social networking.

3 Responsibility and accountability

3.1 Head teachers or principals

3.1.1 should ensure that all existing and new staff are trained and become familiar with this policy and its relationship to the school's standards, policies and guidance on the use of ICT and e-safety;

3.1.2 should provide opportunities to discuss appropriate social networking use by staff on a regular basis and ensure that any queries raised are resolved swiftly;

3.1.3 must ensure that any allegations raised in respect of access to social networking sites are investigated promptly and appropriately, in accordance with the school's disciplinary procedure, code of conduct and internet safety guidelines; and

3.1.4 should ensure there is a system in place for regular monitoring.

3.2 School staff

3.2.1 should ensure that they are familiar with the contents of this policy and its relationship to the school's standards, policies and guidance on the use of ICT and e-safety;

3.2.2 should raise any queries or areas of concern they have relating to the use of social networking sites and interpretation of this policy – with their line manager in the first instance; and

3.2.3 must comply with this policy where specific activities or conduct is prohibited.

3.3 Solihull Council human resources

3.3.1 will advise and support head teachers and line managers on the application of this policy.

3.4 School governors

3.4.1 will review this policy and its application annually (or more frequently as required); and

3.4.2 should ensure that their own behaviour is in line with that expected – as outlined in the governors' code of conduct and in accordance with this policy.

4 When using social media at any time

4.1 Staff must not place a child at risk of harm.

4.1.1 Staff must follow statutory and school safeguarding procedures at all times when using social media.

4.1.2 Staff must report all situations where any child is at potential risk by using relevant statutory and school child protection procedures.

4.2 Staff must not allow their use of social media to affect their ability to do their job in any way.

4.2.1 Social media relationships must be declared with other personal relationships or interests whenever necessary or appropriate.

4.3 Staff must maintain the reputation of the school, its staff, its pupils, its parents, its governors, its wider community and their employers.

4.4 Staff must not contribute or access any social media content which is illegal, discriminatory, sexual, or otherwise offensive when linked in any way to the school. This link could be, as examples, by identification with the school, during the working day, on school premises or when using school equipment. Such behaviours may also result in criminal proceedings.

4.4.1 Staff must recognise that contributing or accessing any social media content which is illegal, discriminatory, sexual or otherwise offensive during personal use could lead to damage to their professional reputation or damage to the reputation of the school. This damage would breach the social media policy. And, again, such behaviours may also result in criminal proceedings.

4.5 Staff must not use social media to criticise or insult their school, its staff, its pupils, its parents, its governors or its wider community.

4.5.1 Staff should be aware that there are other, more appropriate, methods of raising valid concerns about their school and its staff.

4.6 Staff must not use social media to harass, bully or intimidate any pupil, parent, member of staff, governor or other member of the wider school community.

4.7 Staff must not breach school confidentiality.

4.7.1 School staff must follow their school data protection responsibilities when using social media.

4.7.2 Staff must not reveal any other private or confidential school matters when using any social media.

4.8 Staff are responsible for their actions (and its consequences) whenever they use social media.

4.8.1 Staff are responsible for all their social media content.

4.8.2 Staff must understand that social media offers no guarantee of privacy and that any content they produce can be shared more widely by others. A member of staff's professional reputation or the reputation of the school could be damaged by content, perhaps which was intended to be private, being shared more widely than intended.

4.8.3 Staff would still be held responsible for any consequential breach of this policy as they were responsible for producing the original content.

4.9 Staff are responsible for the configuration and use of any personal social media accounts they have. They are responsible for determining the level of security and privacy of all their social media content.

4.10 Staff must raise all doubts, questions and concerns related to social media with school leaders. Staff must seek advice if they are not sure if any particular use of social media (or a related action) is appropriate or would potentially breach this policy. Staff cannot rely on their ignorance or lack of knowledge to defend any breach of this policy.

5 When using social media on behalf of the school

Some schools use social media as a communications channel for their school and to engage with their wider community.

5.1 Staff must be given explicit permission to use social media on behalf of their school by a school leader.

5.2 These staff must follow all related procedures when acting on behalf of the school.

5.3 Staff must have separate user accounts for school use of social media.

5.4 Staff must not use school social media for any personal discussions or for any individual personal matters even if initiated by other members of the school community. Users must be directed to more appropriate communication channels.

6 When using social media as part of working with pupils and students

Some schools are starting to use social media to engage with their own pupils to support learning.

6.1 Staff must ensure that all social media use when working with pupils is sanctioned by the school; only uses explicitly agreed social media; and, follows agreed policies and procedures.

7 When using social media in staff's wider professional life

Social media is a useful tool for engaging and collaborating with the wider education community.

7.1 Staff must be clear that their social media content is personal and not endorsed or supported by their school.

7.2 Staff can identify their school where appropriate but cannot use account names, school branding or anything else that could imply that the content is official school content.

7.3 Staff must be particularly careful to not reveal any details of staff, pupils, parents or other members of the school community that make it possible to identify any individuals.

7.4 Staff must use appropriate behaviour and language at all times. As a guide, this should be similar to that which would be used when taking part in a face-to-face meeting with other education professionals.

8 When using social media in staff's personal life

8.1 The personal use of social media must neither interfere with a member of staff's ability to maintain their professional reputation nor impact on the reputation of the school.

8.2 Staff must take all reasonable steps to ensure the proper separation of their professional and personal lives.

8.2.1 Staff must not use school social networking accounts for personal content.

8.2.2 Staff must respect the wishes and privacy of any other members of their school community with whom they have personal social media contact.

8.3 Staff must not use personal social media with any child with whom they solely have, or have had, a staff/pupil relationship. This includes ex-pupils until they reach the age of 18.

8.3.1 School staff can have social media contact with pupils or ex-pupils where other appropriate relationships exist. As examples, a pupil who is also a family member or a family friend. These relationships must be open and transparent. The member of staff can report these social media relationships to senior leaders for their own protection.

8.3.2 Staff must retain any communications to pupils or ex-pupils rejecting any approaches made on social media and ensure that they are professional in tone. Staff must also consider reporting these to senior leaders to ensure transparency.

8.4 Staff must not use personal social media with anyone with whom they solely have a staff/parent relationship.

8.4.1 Staff at schools can often have more complex relationships than just being a member of staff or a parent. As examples, staff can also be parents (of pupils at the school), in relationships or have friendships with other staff or parents; or also governors. Any member of staff can report any social media relationships to senior leaders for their own protection.

8.5 Staff must make sure that their personal social media activities take into account who they have social media relationships with – particularly any other members of school community – and moderate their social media behaviour accordingly.

8.6 Personal use of social media at school:

8.6.1 School staff can make reasonable personal use of social media during the working day or while at their school. This must not interfere with any work activities.

8.6.2 Staff can only use social media when no pupils are present and during breaks or non-directed time.

8.6.3 Staff can use school devices where social media sites can be accessed using school systems. This use must also follow the school's staff acceptable use policy (AUP).

There is no obligation on the school to make social media sites available to staff.

8.6.4 Staff can only use personal devices with social media while at their school where the use of personal devices is allowed by the school. Again, this use must still follow the school's acceptable use policy (AUP).

9 Excessive use of social media at school

9.1 Staff must not spend an excessive amount of time while at the school on personal use of social media. They must ensure that use of social media does not interfere with their duties.

10 Monitoring use of social media on school equipment

10.1 The school reserves the right to monitor all staff internet use, including when staff are making personal use of social media, on any school systems or equipment. Misuse of social media – even personal use – on school equipment is a breach of the school's acceptable use policy.

11 Disciplinary action over social media use

11.1 All staff are required to adhere to this policy. Staff should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the school, may constitute gross misconduct and lead to summary dismissal.

11.2 Similarly, where there is a serious breach of this policy, action may be taken in respect of other members of staff who are not employees (volunteers) which may result in the termination of their appointment.

11.3 The head teacher should take advice from Solihull Council's human resources team before considering disciplinary action.

12 If you have any concerns

12.1 When using social media, you may have a concern about what you are seeing or being told by another user which has safeguarding implications or may cause harm to the reputation of the school and/or its community. If you have any such concerns you should contact the head teacher, the named safeguarding contact in school, or human resources for advice.

12.2 If a member of staff becomes aware that a pupil (or group of pupils) or parent has made inappropriate/insulting/threatening comments about them, or other staff members, on a social networking site; then they should consider reporting this to the head teacher so that the appropriate process can be followed and support can be offered to the employee.