



## **Larkfields Junior School**

### **Internet, E-Safety and Acceptable Use Policy**

#### **Internet Use**

At Larkfields Junior, pupils and staff have access to the Internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. However, the school and parents have a duty of care to protect children, help them to protect themselves and encourage Internet use that is responsible and safe.

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

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

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

Parents will be sent this policy and details, which form our Acceptable Use Policy (at the end of this document). This can be seen as an extension to the Home School Agreement.

#### **Pupil access to the Internet**

The school encourages use by pupils of the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our pupils will be entering. Children can access the Internet in school via computers and/or iPads.

Benefits to the whole school of effective Internet use include:

- Access to a wide variety of educational resources
- Access to a vast variety of up-to-date information via effective search engines
- Rapid and cost effective world-wide communication
- Gaining an understanding of people and cultures around the globe
- Staff professional development through access to new curriculum materials, experts' knowledge and practice
- Exchange of curriculum and administration data with LA/DfE

- Social and leisure use.
- Greatly increased skills in Literacy, particularly in being able to read and appraise critically and then communicate what is important to others

As pupils gain experience, they will be taught how to use searching techniques to locate and specific information for themselves. Comparisons will be made between researching from different sources of information,

At times, information, such as text, photos etc may be 'downloaded' from the Internet for use in pupils' presentations. Tasks will be set to encourage pupils to view web sites and information with a critical eye.

All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught and the IT Co-ordinator will assist in the dissemination of this information.

### **Dangers to consider**

Some of the dangers we wish pupils to avoid 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 risk of being subject to sexual exploitation by those with whom they make contact on the Internet
- The risk of being subject to radicalisation by those with whom they make contact on the Internet
- The risk of being influenced to act in a different way through online peer pressure
- 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 young person.

It is impossible to eliminate all of those risks completely. It is therefore essential to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school believes that the benefits to pupils from a wider range of learning resources, access to information and increased opportunities for collaboration exceed the disadvantages. However, ultimately, parents and guardians are responsible for setting and conveying the standards that their children should follow when using media and information sources at home and the school must provide the necessary safeguards to manage and reduce these risks in school.

**School Rules**

The school has developed a set of E-safety rules for our pupils to follow. These are listed in the pupil section of the Acceptable Use section below. The rules will be made available to all pupils and will be kept under constant review.

All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

At present, Larkfields Junior School uses AITN's (George Spencer Academy) "filtered" Internet Service, which will minimise the chances of pupils encountering undesirable material.

Larkfields Junior School will only allow children to use the Internet when there is either a responsible adult present to supervise or when children have been given specific permission to use the internet for a specific purpose. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen.

Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils.

Teachers will have access to pupils' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.

**Who is involved?**

Guidelines for acceptable use for pupils should be read and signed by all pupils and their parents on entry into the school and again on an annual basis. One signed copy of the Acceptable Use Policy for pupils should be returned to school and kept in the child's central record folder. Any pupils who have not had the guidelines signed by a parent should not be allowed to access the Internet at school.

All staff, including teaching assistants, office staff, midday supervisors, catering staff, premises staff and student teachers should read and sign the guidelines outlining acceptable use of the Internet for staff upon commencement of employment at Larkfields Junior School. Signed copies of the policy should be returned to and stored with their personal files. A record will be kept on the Single Central Record (SCR) that staff have signed the guidelines. Governors should be familiar with the contents of the policy.

**Sanctions**

It is essential that pupils understand the main aim of the Internet, E-Safety and Acceptable Use Policy is to keep them safe on the Internet. Any pupil found to be breaking the rules should be referred to the IT Co-ordinator, SLT or Headteacher as appropriate and be disciplined in line with the school's behaviour policy. This may involve parents being informed.

Similarly, staff should ensure that they make every effort to protect themselves at all times from the risks associated with the use of technologies and the Internet. Any member of staff found to be contravening the guidelines may, depending on the circumstances, be subject to disciplinary procedures in line with the school's policy and may not have the backing of the Local Authority or the school. In some circumstances, the appropriate authorities may have to be informed.

In addition, if a parent/carer uses the Internet inappropriately in connection with school matters they put themselves at risk of legal action being taken against them.

## **E-Safety**

E-Safety addresses how we use Internet technologies and electronic communications such as mobile phones and wireless technology (including iPads). It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's e-safety policy will operate in conjunction with other policies including those for Anti-Bullying and Child Protection. It will support our efforts to protect children from online grooming and radicalisation.

It is now our responsibility to equip our pupils with the skills and knowledge they need to use technology safely and responsibly whenever and wherever they go online. Although, it seems that children are our primary concern, it is important to recognise that the development of safe and responsible behaviours online extends to staff, parents and carers and members of the wider community. As staff, we have a duty to protect the children in our care but at the same time we are susceptible to risks. There are many recent reports of teachers being harassed or intimidated by new technologies, both in and out of the classroom. Equally there are reported instances of childcare professionals compromising their reputation through social networking sites and other forms of media. Within school, we have access to a range of personal and sensitive data and we must ensure that we use technology and systems securely at all times.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from the provider including the effective management of content filtering

The school has developed a sequence of lessons and assemblies designed to educate children so that they understand how to keep themselves safe online. The school also communicates with parents so that they know how to keep children safe on the internet at home. This is done via updates on the school newsletter, information on the school website and parent meetings.

## **Prevent**

At Larkfields Junior, we recognise the unique part ICT and, specifically internet access, has to play in meeting the requirements of the Prevent Duty. Given that children and young people can be out at risk of online radicalisation, the school has a system for teaching children about online safety. This would include being aware that not everything they read on the internet is true and that there is a risk of others trying to influence what young people think. As far as possible, the school will work with its IT support service to ensure that children cannot gain access to websites that put them at risk of radicalisation.

Teachers and support staff have also been trained to listen out for indicators of children being put at risk online.

## **Cyber bullying**

In accordance with our anti bullying policy, the school educates children about the risks of cyber bullying, why it is wrong and how to report it.

Definition:

Cyber bullying is the use of Information Communications Technology (ICT) particularly mobile phones and the internet, deliberately to upset someone else. This can take the form of:

- Threats and Intimidation
- Harassment and Stalking
- Exclusion (of an individual from groups and sites)
- Identity theft, unauthorised access and impersonation
- Publicly posting, sending forward personal or private information or images
- Manipulation (pressure to arrange a meeting or to give out personal information).

The Education and Inspections act of 2006

The power to regulate pupil's behaviour out of school works as a defence for school staff to confiscate items e.g. mobile phones.

Head teachers are specifically granted powers that enable them to police cyber-bullying carried out by pupils even at home.



## Larkfields Junior School

### E-Safety – Acceptable Use Policy

#### *Pupils*

We all have access to the Internet, either at home or at school. Everyone is really positive about the Internet and how important it is in our day to day lives. We can use the Internet to help us learn, make homework more interesting, for entertainment and keeping in touch with our friends.

**These rules will help me stay safe on the Internet and be fair to others, at school and at home.**

- I will only use the school computers and iPads for school work or homework.
- I will login only with my own username.
- I will keep usernames and passwords, at school and at home, private and will not share them with other people.
- If I use general school passwords at home for web based software, e.g. mymaths, I will use this account appropriately.
- I will only edit or delete my own files and will not look at or change other people's files without their permission.
- I will only use the Internet under the supervision of an adult.
- I will not bring files in on memory sticks into school without permission and understand that if I do they will be checked with an anti-virus scanner. I will make sure that my memory stick only contains items of schoolwork or homework.
- I will not use any chat or social network sites at school, unless supervised by an adult as part of a learning opportunity.
- I am aware that some websites and social network sites have age restrictions and should avoid using these sites at home.
- I will only email people I know, or those my parent/carer or teacher has allowed me to.
- Any electronic messages I send will be polite, friendly and sensible.
- I will not open an attachment or download a file unless I know and trust the person who has sent it.
- I will not share any personal details over the internet such as my name, address, telephone number, name of school or photographs of myself.
- I will not arrange to meet anyone I have met over the Internet and understand that I must tell an adult if anybody suggests this.
- If I receive a message I do not like or see something that I think might be wrong, makes me unhappy or uncomfortable I will tell my parent/carer, if I am at home, or my teacher, if I am at school.
- I understand that the school can check my school files and the Internet sites I have visited at school at any time.

- When I am using the internet to find information, I will check that the information is accurate as I understand the work of others may not always be truthful
- I am aware that I should not give in to peer pressure on line.
- I will tell an adult if somebody online tries to make me do things or believe things I am not used to.

## Information for parents/carers

- Parents/carers may take photographs of their own children at school events, such as sports day, concerts and musical events. This rule will be re-evaluated on a regular basis and parents/carers will be informed if it changes. Parents should switch off mobile phones when visiting school to help in lessons.
- Photographs of children are not to be taken in the swimming pool.
- Any photographs containing images of other pupils should not be published on social networking sites, the Internet or sent by email.
- Some chat and social networking sites e.g. Facebook (age 13) have age restrictions. If you allow your child to use these sites, please be aware that any problems that may arise can upset children. School may attempt to assist with a problem up to a certain level but ultimately cannot be responsible for content that is written away from the school site. In extreme cases, the school may pass information onto the Police or appropriate authority.
- We suggest that parents using the Internet at home with children adopt a similar set of safety rules to those agreed at school.
- Parents should be aware that online grooming and radicalisation is a growing problem. They should watch out for this and tell police or school if they have evidence of a problem.
- **Parents/carers should be aware that inappropriate use of the internet in connection with school matters could result in legal action being taken including involvement of the police. This could include negative or inappropriate comments about the school or school staff on social media.** Complaints about school, if they occur, should be made in line with the school complaints procedure. See website for further information.



I have read and agree to all the rules for staying safe on the internet. I have talked them through with a parent/carer and understand what each one means. I know that it is my responsibility to stay safe on the internet but that my parents/carers and teachers are there to help me and give me advice too. I understand that if I break any of the rules, I will be disciplined in line with the school behaviour policy and my parent/carer might be informed.

Child's name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Parent/carer's signature: \_\_\_\_\_

Date: \_\_\_\_\_



## Larkfields Junior School E-Safety - Acceptable Use Policy Staff

The purpose of Internet use in school is to assist pupils to achieve increasingly high standards, to support the professional work of staff and to enhance the school's management. Following these rules will help us to protect ourselves against any risks.

- I will make sure that pupils are supervised as closely as possible when using the Internet or have been given clear instructions regarding what to do in independent study.
- I will not take photos or videos of children on my mobile phone
- I will only use school equipment (cameras and I-pads) to take photographs or videos for school purposes.
- I will only save sensitive work to a school provided memory stick/laptop that has password protection.
- I will only publish photographs/videos of children on displays, letters or the school website when school has received written permission from parents/carers.
- I will not publish a child's full name alongside a photograph/video of them.
- I will use my school email address for work purposes (including contacting other members of staff regarding planning, assessment etc) and not my personal email address.
- I will ensure that if I wish to transfer any confidential data from location to location, I will either email it to myself or save it on a password protected memory stick.
- I will not share my school passwords with other staff. A central list of staff passwords will be kept by the Head Teacher.
- I understand that I should not befriend a pupil, parent, future parent or ex-pupil on a social networking site. If I do, I understand that I might not have the backing of the LA should an allegation be made.
- I will endeavour to check the suitability of online resources before using them and I am aware that these can change at short notice.
- I will not post information or photographs about myself or school related matters on social networking sites that I would not want employers, colleagues, parents or pupils to see or might compromise my professional position.

- I will only use personal email or social networking sites at school when children are not present in hours when I am not legally contracted to be on the premises.
- I will not browse, download or send to colleagues any material which could be considered offensive.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not copy or download any inappropriate material onto my school laptop/iPad.
- I will be vigilant to any electronic evidence or pupil conversations that might suggest pupils are being groomed, radicalised put at risk or bullied via the internet or through modern technologies. I will report such suspicions to the Headteacher.
- I will report any accidental access to, or receipt of any inappropriate materials, or filtering breach on the part of myself or pupils to the head teacher.
- The Headteacher/ICT co-ordinator will keep an internal log of incidents that are of concern with regard to E-Safety. This may be confidential.
- I will embed the school's E-safety curriculum into my teaching.



---

## Larkfields Junior School E-Safety - Acceptable Use Policy Staff

I understand that it is my responsibility that I remain up to date and read and understand the school's E-Safety Policy. I understand that all Internet usage and network usage can be logged and this information could be made available to my manager on request. I have read the guidelines on acceptable use for staff and agree to abide by all the points. I am aware that failure to do so could result in disciplinary procedure in line with school policy.

Signature \_\_\_\_\_ Date \_\_\_\_\_

Full name \_\_\_\_\_

Job Title \_\_\_\_\_

|  |   |   |
|--|---|---|
|  <p><b>DON'T GIVE OUT PERSONAL INFORMATION</b></p> <p>Don't give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.</p>  |  <p><b>KNOW WHO YOU'RE TALKING TO</b></p> <p>Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.</p> |  <p><b>ONLY OPEN MESSAGES FROM SOURCES YOU TRUST</b></p> <p>Accepting emails, messages, or opening files, images or texts from people you don't know or trust can lead to problems – they may contain viruses or unpleasant messages!</p>    |
|  <p><b>NOT EVERYTHING ONLINE IS TRUE</b></p> <p>4. Someone online might lie about who they are and information on the internet may not be true. Always check information by looking at other websites, in books, or with someone who knows. If you like chatting online it's best to only chat to your real world friends and family.</p> |  <p><b>SPEAK TO SOMEONE IF YOU FEEL UNCOMFORTABLE.</b></p> <p>5. Tell a parent, carer or a trusted adult if someone, or something, makes you feel uncomfortable or worried, or if you or someone you know is potentially being radicalised online.</p>   |  <p><b>PROTECT YOUR ONLINE REPUTATION</b></p> <p>Use the tools provided by online services to manage your digital footprints and 'think before you post.' Content posted online can last forever and could be shared publicly by anyone.</p> |
|  <p><b>KNOW WHERE TO FIND HELP</b></p> <p>Understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it's never too late to tell someone.</p>  |  <p><b>DON'T GIVE IN TO PRESSURE</b></p> <p>Don't be pressured into doing something you know is wrong. If it's something you wouldn't tell your friends and family about, it's probably not something you should be doing!</p>   |  <p><b>PROTECT CHILDREN AND THE VULNERABLE</b></p> <p>Children and vulnerable adults can be contacted by bullies and people who want to groom/radicalise or seek to abuse them.</p>  |
|  <p><b>CHECK THAT CONTENT IS APPROPRIATE</b></p> <p>Age-inappropriate or unreliable content can be available to children.</p>   |  <p><b>KEEP IT SAFE</b></p> <p>Use safety tools on social networks and other online services, eg Facebook privacy settings.</p>  |  <p><b>CONDUCT</b></p> <p>Children may be at risk because of their own behaviour, for example, by sharing too much information.</p>  |