

# **Smithy Street Primary School**

## **Internet Acceptable Use, E-safety and Social Media Policy**



**APPROVED BY STAFF AND GOVERNORS JUL 2018**

## **Part 1:**

### **Internet Acceptable Use/ E-Safety**

- A: Introduction
- B: Using the internet with pupils
- C: Using the internet with staff

## **Part 2:**

### **Social Media**

- A: Introduction
- B: Scope and definitions
- C: Key Principles
- D: Roles and responsibilities
- E: Safer Social networking practices
- F: Responsibilities when using social media
- G: Access to inappropriate images
- H: Social Media within the curriculum
- I: Teaching of social networking
- J: School Social Media websites
- K: Cyberbullying and trolling
- L: Sexting
- M: The Prevent Duty
- N: Personal use of social media by parents and carers
- O: Complaints procedure
- P: Breaches of policy and other issues
- Q: Associated reading

## **Part 3:**

Pupils' agreement and rules for using the Internet at Smithy Street and at home

Letter to parents: Using the internet at Smithy Street and at home

Staff agreement for Internet use at Smithy Street, Social Media conduct and Data Protection

# Part 1: Internet Acceptable Use/ E-Safety

## A: Introduction

### ***The Internet***

The Internet and related technology including e-mail and social media have become a rich and vital part of education, work and home life. It has transformed the way information is used and transmitted in all aspects of our lives. This powerful technology is always developing, changing and growing, and whilst this is exciting it also presents challenges and dangers that we must address.

### ***What is an acceptable use policy?***

We are committed to using the Internet and all it offers in the most effective and appropriate way at our school, for the benefit of our pupils, staff and community. To this end, we have developed this Internet Acceptable Use/ E-safety policy, to ensure that all members of our school community understand what is expected of them when they use the Internet in the learning environment. Our policy consists of:

- Statements outlining our school's approach and attitudes towards using the Internet
- Clear guidelines and rules for acceptable use
- Internet Acceptable Use and Social Media Agreements, to be signed annually by pupils in KS2 acknowledged by staff.
- A letter for parents outlining our policy, to be sent out at regular intervals.

This policy should be read in conjunction with other relevant school policies, in particular: Child Protection Policy, Behaviour and anti-bullying policy, Safer Recruitment Policy, Code of Conduct, Disciplinary Code, Social Media Policy (part 2 of this document) , Data Protection Policy and Equalities Policy.

### ***Roles and Responsibilities***

Members of the school community have different roles and responsibilities when it comes to using the Internet at school.

<b><i>Role</i></b>	<b><i>Responsibilities regarding use of Internet in school</i></b>
<i>Head teacher</i>	To monitor this policy and ensure it is updated regularly and agreed with all staff
<i>Computing Coordinator</i>	To develop the use of the Internet as a teaching and learning tool across the school To keep up to date with developments in Internet issues as they relate to education, and keep staff informed.
<i>ICT Technician</i>	To ensure that there is adequate( wireless) internet access throughout the school To ensure that adequate Anti-virus software installed and is functioning well To supply user profiles and email addresses to all staff
<i>Class teachers/ Teaching assistants</i>	To ensure that pupils use the Internet purposely and with adult supervision at all times. To know how to deal with incidents involving unsuitable material or situations where pupils feel uncertain or unsafe when using the Internet at school To understand and follow the staff rules for internet use at Smithy Street, Social Media conduct and Data protection
<i>Governing body</i>	To agree this policy and review it on a regular basis
<i>Pupils</i>	To understand the school Internet Acceptable use/ E-safety policy and abide by the rules for pupils
<i>Parents and carers</i>	To be aware of the school Internet Acceptable use/ E-safety policy
<i>Other community users</i>	To understand the school Internet Acceptable use/ E-safety policy and abide by the rules for all users

### ***School Internet provision***

The school, in conjunction with LB Tower Hamlets provides a suitable Internet connection, with broadband capabilities and wireless access.

The school used the standard LEA Internet Service Provider, which is Virgin (Atomwide Service), a part of the London Grid for Learning Broadband consortium. Virgin provides an always-on broadband connection at speeds up to 20MB.

### ***Content filter***

LGFL use a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.

Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

### ***Downloading files and applications***

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

### ***Portable media and hard drive devices***

Portable media such as USB flash drives, memory sticks and portable hard drive devices are a common way of introducing a virus or other undesirable agent into a school computer system.

Staff should take care that files from other computers outside the school are checked for virus contamination before they are used on the school system.

Pupils are not allowed to use USB flash drives, memory sticks and portable personal hard drive devices brought from home.

### ***Security and virus protection***

The school subscribes to the LGFL program Sophos, which is run on the server. The software is updated regularly by our ICT Technician. Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT Technician by creating an online ticket on the school website.

### ***Legal issues***

Our school is aware of the data protection law as it affects our use of the Internet, both in administration and teaching and learning.

We adhere to the Government Guidelines on Data protection. Further guidance can be found in the school's Data Protection policy.

Staff and pupils must understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

## **B: Using the Internet with pupils:**

We believe it is our responsibility to prepare pupils for their lives in the modern world, and the internet is an unavoidable part of that world. At our school we are committed to teaching pupils to use the Internet effectively and appropriately in all aspects of their education.

### ***Safety through supervision***

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always supervised by an adult when using the Internet, and computers and Ipads with Internet access should be carefully located so that screens can be seen at all times by all who pass by.

### ***Internet clubs and after school provision***

We want to ensure that all our pupils have access to the Internet, particularly where this will directly support their learning. To this end, we may provide additional access and support for pupils through ICT clubs. **Pupils will not have unsupervised access to the Internet at any time.**

### ***Using the Internet for learning***

The Internet is an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

We teach all of our pupils how to find appropriate information on the Internet, and how to ensure, as far as possible, that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- If a member of staff wishes to access a website that is blocked by LGFL, and if it is deemed an appropriate site for educational use, the member of staff will raise a ticket for ICT technician to unblock the site, quoting a specific date and for how long the site needs to remain unblocked. The ICT technician will re-block the site after the date indicated by the member of staff and close the ticket to confirm this has been done. This must be agreed to by the Headteacher in advance.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

## **Teaching safe use of the Internet**

The Computing Curriculum which was introduced in September 2014 has a strand called E-Safety, in which children are taught how to stay safe online, We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, we also use the **Kidsmart safety code** to support our teaching in this area:

(Kidsmart has been developed by the Childnet charity, and is endorsed by the DfS)

<http://www.kidsmart.org.uk>

The main aspects of this approach include the following five SMART tips:

- **Safe** - Staying safe involves being careful and not giving out your name, address, mobile phone number, school name or password to people online.
- **Meeting** someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present.
- **Accepting** e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages.
- **Remember** someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation.
- **Tell** your parent or carer if someone or something makes you feel uncomfortable or worried.

## **Suitable material**

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check and monitor the suitability of websites when using them in teaching.

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than ban Internet use apart from strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time, at out-of-school-hours provision, and at home.

**There is a selection of links to such resources available for children and parents to see on the school website [www.smithystreet.org.uk](http://www.smithystreet.org.uk).**

## **Unsuitable material**

Despite the best efforts of the LEA and school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Technician and Head teacher
3. Logging the incident
4. Discussion with the pupil about the incident, and how they might avoid similar experiences in future

## **Deliberate misuse of the Internet facilities**

Pupils in Key Stage 2 are asked to sign the '*Pupils' Agreement and Rules for Using the Internet at Smithy Street and at home*' (see part 3).

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse, in line with our school behaviour/ anti-bullying policy.

## ***E-Mail***

E-Mail is a valuable and stimulating method of communication which plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mails, and how to use it appropriately and effectively. We may create pupils' emails for the purpose of this.

Pupils are not allowed to access personal e-mail using school Internet facilities, due to the quantity of unsolicited e-mail (Spam), unsuitable content and virus threats associated with commercial e-mail accounts. The school may be able to arrange pupil school emails for educational purposes.

## ***Social Media***

Many forms of social media are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas.

Social media, including emails, YouTube, blogs and discussion boards present a range of personal safety and privacy issues for young people.

We only use safe resources and follow strict guidelines and materials, such as those offered by Kidsmart, to teach children how to use social media in an age appropriate and safe way.

Pupils are only allowed to access any social media, YouTube, blogs, discussion boards etc. under strict supervision by teachers, and only where it suits an educational purpose and is part of a planned activity.

More information and guidance on the use of social media by staff can be found in Part 2 of this document

## ***Online bullying and harassment***

Online bullying and harassment via social media such as WhatsApp and Snapchat are potential problems that can have a serious effect on pupils.

Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:

- Supervised access to emails, YouTube, public blogs, and discussion boards
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of safe sources

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

## ***Contact details and privacy***

Parents/ carers are asked to sign a digital Image consent form when enrolling in the school. Where consent has not been given, the teacher will be informed. Pupils' personal details, identifying information, alongside images should never be used for any public Internet-based activity.

Pupils are taught that sharing this information with others can be dangerous.

More information and guidance on the use of social media, handling sensitive information and images can be found in Part 2 of this document and the Data Protection policy.

## ***School and pupil websites – pictures and pupil input***

As part of the curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

More information and guidance can be found in Part 2 of this document.

## **Using the Internet with staff:**

### ***Introduction***

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion on educational topics and news.

It also provides an efficient way to access information from the DfE and other government agencies and departments that will help staff to keep abreast of national and local developments.

There are also numerous opportunities for staff to access INSET and Continuing Professional Development activities using the Internet and e-learning resources.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

### ***Availability***

To enable staff to make full use of these important resources, the internet is available to all staff for professional use. Staff may use the internet for personal use at breaktimes, but only when computers are not needed for education purposes. The use of the school website for social media, apart from emails, is not permitted

Staff must obtain the appropriate log on details and passwords from the ICT technician. Only LGFL school emails should be used for work related purposes.

### ***Staff agreement***

All staff using the school Internet facilities have signed a '*Staff agreement for Internet use at Smithy Street, Social Media conduct and Data Protection*'

There are serious implications for staff who deliberately misuse the school Internet facilities, which could result in disciplinary action.

There are also LEA staff rules for Internet use within the LEA. It is a condition of employment that these rules are followed. The LEA staff rules are appended.

### ***Professional use***

Staff model good Internet use where pupils are present, as part of our ongoing commitment to encouraging safe and appropriate Internet use by our pupils both in school and at home.

Staff who need support in using the Internet, or who would like INSET in using it more effectively can ask for support from the ICT technician or Computing co-ordinator

Staff should ensure that they represent the school in a professional and appropriate and confidential way when sending e-mails, contributing to online discussions or posting to public websites using school facilities.

More information and guidance on the use of social media, handling sensitive information and images can be found in Part 2 and the Data Protection policy.

### ***E-mail***

We recognise that e-mail is a useful and efficient professional communication tool, and we encourage staff to use it where appropriate for communicating with colleagues, organisations, companies and other groups.

Staff may access private e-mail accounts during the availability periods outlined above for personal use, but must be careful when downloading any attachments, pictures or other material onto school computers, or onto the school network area. Only LGFL school emails should be used for work related purposes.



## Part 2: Social Media

### A: Introduction

This policy and guidance document recognises that new technologies are an integral and growing part of everyday life and that they make an important contribution to teaching and learning opportunities in Smithy Street Primary School. This policy also recognises that in the light of the rapid evolution of social networking technologies, Smithy Street Primary School requires a robust policy framework so that all children and adults working in school are aware of the school's expectations and the rules they are expected to follow when using social media both inside and outside of the school environment.

This policy is designed to ensure that all adults use social media responsibly in order to safeguard the school, its pupils, staff, school governors and members of the wider school community. It is crucial that children are safeguarded and that parents, pupils and the public at large have confidence in the school's decisions and services. Responsible use of social media will ensure that the confidentiality and privacy of pupils and members of staff are maintained and that the reputation and integrity of the school and the Local Authority are protected.

This policy should be read in conjunction with other relevant school policies in particular, the school's Child Protection Policy, Safer Recruitment Policy, Code of Conduct, Disciplinary Code, Internet Acceptable use/ E-Safety Policy, and Equalities Policy.

This policy takes into account the provisions of the DfE's statutory advice for schools on Keeping Children Safe in Education, the non-statutory guidance on the Prevent Duty and the Briefing Note to schools on "How Social Media is used to encourage travel to Syria and Iraq". It also takes into account the Government's statutory guidance issued under s29 of the Counter -Terrorism and Security Act 2015.

### B: Scope and definitions

This policy applies to all adults working in Smithy Street Primary School and who provide services for or on behalf of the school including employees (teaching and non-teaching staff), self-employed staff, trainee teachers and any other trainees, apprentices, agency staff, external consultants, governors and volunteers.

This policy covers the personal use of social media as well as the use of social media for school purposes (whether official or not), including the use of websites hosted and maintained on behalf of the school.

This policy covers the use of social media and personal blogs and any posts made on other people's blogs and to all on line forums and notice boards. The guidance, rules and principles set out in this policy must be followed irrespective of the social media platform or medium or any new future social media platform.

In this policy, the following definitions apply:

- Social media - means any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. Social media includes but is not limited to, online social forums such as Twitter, Facebook and LinkedIn and also covers blogs, chatrooms, forums, podcasts and video-image-sharing websites such as YouTube, Flickr, Reddit, Instagram, Snapchat and Tumblr, although this list is not exhaustive. The internet is a fast moving technology and it is impossible to cover all examples of emerging social media in this policy.

- Adults/adults working in school - means all members of staff (including teaching and non-teaching staff) who work in Smithy Street Primary School as an employee or on a self-employed basis. It also includes trainee teachers, other trainees and apprentices, volunteers, agency staff, external consultants and school Governors.
- Information - means all types of information including but not limited to, facts, data, comments, audio, video, photographs, images and any other form of online interaction.
- Inappropriate information - means information as defined above which any reasonable person would consider to be unsuitable or inappropriate in the circumstances and taking into account the adult's position within the school.
- The school and the wider school community - means Smithy Street Primary School, its pupils, all adults working in school (as defined above) parents/carers of pupils, former pupils, the Local Authority and any other person or body directly or indirectly connected with the school.

## C Key Principles

Adults have an important role to play in equipping the school's pupils to stay safe online, both in school and outside of school. Adults therefore need to be aware of the risks associated with the use of social media and in particular about the provision and sharing of information in the social media arena.

Adults must not, whether deliberately or inadvertently and whether in their working time or in their personal time, provide, publish or share **inappropriate information** on or via any social media platform or medium about the school and the wider school community or about themselves that could **damage the reputation of the school**.

Adults are **accountable for and must take responsibility** for all information published or shared by them on social media websites and for any views expressed by them on any such sites, whether in their working time or in their personal time and which may come into the public domain. Adults should be aware that their use of social media and any information published by them may be monitored by the Head teacher, members of the school's senior leadership team and/or members of the school's Governing Body.

All adults who provide, **publish or share information which causes harm or distress or which has the potential to cause harm or distress or to cause reputational damage to the school** and the wider school community will be dealt with as appropriate by the Head Teacher in accordance with the relevant school policy/procedure. This may include action being taken under the school's Safeguarding Policy (which could lead to a referral to the Local Authority and/or the Police) and it could also lead to disciplinary action being taken under the school's Disciplinary Policy which, in serious cases may lead to dismissal without notice.

The principles which underpin this policy are:-

- adults are responsible for their own actions and behaviour and must avoid any conduct which would lead any reasonable person to question their motivation and intentions;
- adults must be conscious at all times of the need to keep their personal and professional lives separate; adults must not put themselves in a position where there is a conflict between their work and personal interests;
- adults must work and be seen to work, in an open and transparent way;
- adults must continually monitor and review their own practices in terms of the continually evolving world of social networking and social media and ensure that they consistently follow the rules, principles and guidance contained in this policy.

## D: Roles and Responsibilities

The Head teacher and the Governing Body will:

- ensure that all adults working in school are familiar with this policy and any related policies;
- take all reasonable steps to enable adults working with children to work safely and responsibly and to support safer working practice in general with regard to the use of the internet and other communication technologies;
- take all reasonable steps to assist adults to monitor their own practices and standards with regard to the use of the internet and other communication technologies ;
- set clear rules in relation to the expected standards of behaviour relevant to social networking for educational, personal or recreational use;
- give a clear message that unlawful or unsafe behaviour or practice is unacceptable and that where appropriate, disciplinary, legal and/or other action will be taken;
- ensure that all concerns raised in relation to the accessing of social media or social networking sites are investigated promptly and appropriately;
- take all reasonable steps to minimise the risk of misplaced or malicious allegations being made against all adults working in school;
- take all reasonable steps to prevent adults working in school abusing or misusing their position of trust.

Adults working in school must:

- ensure they are familiar with the contents of this policy;
- adhere to and apply the rules, guidance and principles in this policy in all aspects of their work and in their personal time;
- act in accordance with their duties and responsibilities under this policy and the statutory/ non statutory advice and guidance referred to;
- raise any concerns or queries in connection with this policy with the Head teacher;
- attend any training provided or facilitated by or the school in relation to the use of the internet or any other communication technologies;
- never, in any circumstances, abuse or misuse their position of trust.

### **E: Safer social networking practice**

Adults should be aware of the risks and dangers of revealing personal information on social networking sites. Disclosing personal information on social networking sites may compromise an adult's personal safety and security and it also increases the potential for identity theft by third parties and increases the potential for pupils, their families or friends having access to adults outside of the school environment. Personal information includes information such as a home address, home and mobile telephone numbers and details relating to place of work.

Adults, particularly those new to the school setting, must **review their social networking sites** when they join the school and should ensure that they have the **appropriate privacy settings** in place to ensure that information available publicly about them is appropriate and accurate. This should include reviewing any photographs or images that may cause embarrassment to them and/or to the school and the wider school community.

### **F: Responsibilities when using social media**

Adults should take responsibility for their personal telephones and any personal electronic devices and must keep their personal telephone numbers, login details, passwords, pin details and personal email addresses private and secure.

Where there is a need to contact pupils or parents the school's email address and/or mobile) telephone should be used. Adults must not use their personal telephones or email accounts for these purposes, unless this is unavoidable in a case of an emergency.

Adults must understand who is allowed to view the content on their social media pages of any websites they use and how to restrict access to certain groups of people, including pupils. Appropriate privacy settings are vital.

Adults **must not request, or respond to a request for any personal information from or about a pupil** at the school.

Adults must not engage in conversations about pupils with their parents or carers or with any other person by any form of social networking or social media unless they have the express permission of the Head teacher to do so.

Adults must only use the official school website for communicating with parents or to enable pupils to communicate with each other **using authorised and previously agreed protocols**. Any communications with pupils (including by email, telephone or text communications) outside of agreed protocols will be treated as a very serious conduct matter and may lead to disciplinary action up to and including dismissal. It may also lead to a criminal investigation.

Adults must never "follow" or allow themselves to be "followed", or make a "friend" of or have **any contact with a pupil at the school on any social networking site**. The only exception to this rule is where the pupil is a member of the adult's family provided agreed protocols are followed and the family relationship has been identified to and acknowledged by the Head teacher.

In cases where a pupil is a family member, adults must be aware that if the family relationship has not been identified and acknowledged by the school, contact through social networking or social media will be a breach of this policy (and therefore will be treated as a serious conduct issue). Adults must be clear that such contact could also be misconstrued as being part of a grooming process. Since family relationships can be easily identified and recognised, **adults must notify the Head teacher of any family relationship with a pupil** so that the position can be formally acknowledged, discussed and recorded.

Adults must never use or access the social networking sites or social networking pages of pupils at the school unless the pupil is a member of the adult's family and the family relationship has been acknowledged and discussed in advance with the Head teacher.

Adults have a duty to report any pupil social networking pages as all Smithy Street Primary pupils are under the age of 13, which is the recommended age for the majority (but not all) social networking sites.

Adults must be cautious about any form of social networking contact with former pupils particularly where siblings or other relatives continue to attend the school or may attend the school in future.

**Adults must not follow or be followed by parents/carers of pupils, accepting parents of pupils as friends on Facebook or having contact with parents/carers on any social networking site**. Adults must be mindful at all times of the boundaries between their work and personal life in accordance with the Key Principles detailed in this policy.

Adults should also be cautious when inviting work colleagues to be friends on social networking sites. Social networking sites can blur the boundaries between work and personal lives and it may be difficult to maintain professional relationships.

Adults must not use social media and the internet in any way to attack, insult, criticise, abuse or defame pupils, family members of pupils, colleagues, governors, the school in general and the wider school community. Adults must always show respect to others when using social media.

Adults must **never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring them or the school and the wider school community into disrepute or which could be interpreted as reflecting negatively on their professionalism.**

Adults must not represent their **personal views** on any social media forum as being in any way **linked to the school or being the views** of the school.

**Photographs, videos or any other types of images of pupils and their families or images depicting staff members or where the school can be identified must not be published on personal social media.**

Teachers must at all times be mindful of the **Teachers' Standards** applicable to their profession and act in accordance with those standards. The Teacher Standards make clear that a teacher must uphold public trust in the profession and maintain high standards of ethics and behaviour both within and outside of school, by ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law. Any breach of the Teacher Standards will be considered a matter of misconduct and may lead to formal disciplinary action being taken.

Adults must devote the whole of their time and attention to their duties during working hours. **Personal use of the internet is not permitted during working hours** and any breach of this provision will be regarded as a conduct matter and disciplinary action taken as appropriate. It is permitted to use the internet for personal reasons, including emails during break times. It is not permitted to use the school internet for personal social media use.

**Confidentiality issues** must be considered at all times in relation to social networking and the use of social media. All employees are bound by a common law duty of fidelity. There are also other laws which protect the school's confidential information which adults working in school may have access to during the course of their work. Confidential information includes but is not limited to person identifiable information for example pupil and employee records, information protected by the Data Protection Act and information provided by the school in the expectation of confidence including information about the school, pupils and the families of pupils, the school's staffing or business plans, and any other commercially or politically sensitive information.

Adults must ensure that they do not **provide, publish share or otherwise disclose any confidential information about themselves or about the school** and the wider school community in breach of their duty of fidelity or in breach of other laws relating to confidentiality and privacy including the Human Rights Act 1998, and the Data Protection Act 1998.

Adults must ensure they understand their obligations under the Equality Act 2010 and under the school's Equality Policy. Breaches of the Equality Act 2010 or the school's Equality Policy through the use of social networking or social media will be considered a serious conduct matter which may lead to disciplinary action up to and including dismissal. Adults should also be aware that they could be held personally liable for their own discriminatory actions under the Equality Act 2010. If, for example an adult were to harass a co-worker online or engage in a discriminatory act in relation to one of the

protected characteristics under the Equality Act 2010, this may result in legal action being taken against them.

Adults should also be aware that there are other laws relating to libel, defamation, harassment and copyright which may apply to information, published or posted by them on social media and which could lead to legal action being taken against them.

All concerns about communications, social contact or social media/social networking issues must be raised with the Head teacher immediately.

### **G: Access to inappropriate images**

There are no circumstances which justify adults possessing **indecent images of children** whether in working time or in an adult's personal time. Adults who access and/or possess links to such material or websites will be viewed as a significant and potential threat of harm to children. Appropriate action will be taken against the adult concerned in these circumstances which, for the avoidance of doubt, will include action under the school's Safeguarding Policy (which could lead to police and Local Authority involvement) and disciplinary action (which could result in dismissal without notice on the grounds of gross misconduct). Where indecent images of children are found by any adult, the Head teacher must be informed immediately.

Adults must not use **equipment belonging to the school to access pornography or adult or explicit material** of any kind. Personal equipment containing these images or links to them must not be brought into school. If any adult uses school equipment or personal equipment in school to access pornography or links to it, this will raise serious concerns about the suitability of the adult concerned to work with children. This will lead to an investigation and may lead to disciplinary action and any other action considered appropriate in the circumstances.

Adults must ensure that pupils **are not exposed to any inappropriate information, images or web links**. The school will endeavour to ensure that internet equipment used by pupils has the appropriate controls with regards to access. Any concerns or potential issues identified by any adult must be **reported** immediately to the ICT technician as well as the Head Teacher or member of SLT.

Where any form of unsuitable material is found, which may not be illegal but which could or does raise concerns about an adult working in school, the Head teacher should be informed immediately. The Head teacher may take HR or legal advice on the appropriate way forward.

### **H: Social Media within the Curriculum**

It is a requirement of the National Curriculum that pupils: "are responsible, competent, confident and creative users of information and communication technology"

In Key Stage 1, pupils should be taught to: "Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies"

In Key Stage 2, pupils should be taught to: "Use technology safely, respectfully and responsibly; recognise acceptable behaviour; identify a range of ways to report concerns about content and contact."

### **I: Teaching of Social Networking**

Children may access to Social networking platforms such as email, or blogging websites as a means of safe social networking and strictly supervised as part of the computing

curriculum. Appropriate and respectful behaviour on these platforms is explicitly taught and concerns of misuse are to be forwarded to the Computing Co-ordinator for investigation and action where necessary. Parents will be made aware of more serious cases.

The computing curriculum provides opportunities for children to be reminded of their 'digital footprints' as well as their responsibilities online and where to report concerns. Depending on the privacy policy of the company, it is a violation for users under the age of 13 to have or use social media accounts. Therefore, at no times will children have direct access to school or personal social media accounts.

## **J: School social media websites**

There must be a strong pedagogical or business reason for creating an official school social media/social networking website including websites to communicate with pupils. Adults must not create websites for reasons which could expose the school to unwelcome publicity or which could cause reputational damage to the school. The matter must have been discussed, authorised and agreed with the Head teacher in advance of any school website, including social media websites, being created.

Adults must at all times act in the best interests of the school and the pupils when creating, participating in or contributing to the content of any website created on behalf of the school.

Adults with access to the school social media accounts must ensure that content posted on the accounts reflects the **respectful and inclusive** ethos prescribed by the school. Adults using the accounts on behalf of the school may not comment on or reply to any statement that could bring the school's reputation into disrepute. Furthermore, adults recognise that content posted is a permanent representation of the school and content/interactions with community members will be monitored.

**Photos of pupils may not be stored on personal devices and must be checked against the photo permission list before posting photos of the children online to ensure privacy is respected at all times. Photos of pupils will not be posted with names attached.**

The work posted to the accounts reflects the learning inside the school and must uphold the high standards set within the school.

Use of the **school social media accounts** ( such as the school blog, school website and text messages) must adhere to Child Protection and Data Protection Policy at all times. Adults with access may only post content during non-teaching time, unless using the accounts with pupils for the purpose of teaching social media.

Access to accounts must never be shared with anyone other than those designated and each member of adults with access is accountable for their use of the school social media as per the disciplinary policy.

The school website will serve as the main communication tool where key policies and statutory documents are shared. All significant events in the school community and outstanding examples of pupil's work may be shared on the school website.

## **K: Cyberbullying and Trolling**

“Cyberbullying” can be defined as “the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.’

If cyberbullying takes place, adults **should keep records of the abuse, texts, e-mails, website or instant messages** and should not delete the said texts, e-mails or messages. Adults are advised to take screen prints of messages or web pages and to be careful to record the time, date and location of the site.

Trolling” can be defined as “circumstances where a person sows discord on the internet by starting arguments or upsetting people by posting inflammatory messages in an online community with the deliberate intent of provoking readers into an emotional response;’

If trolling occurs, adults are advised to take screen prints of messages and should not delete any evidence of trolling.

Adults must report all incidents of cyberbullying and/or trolling to the Head teacher. Any such incidents will be taken very seriously. Adults who have been subjected to cyberbullying or trolling may wish to seek the support of their trade union or professional association representative.

## **L: Sexting**

‘Sexting’ is one of a number of ‘risk-taking’ behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with ‘online’ activity can never be completely eliminated.

However Smithy Street Primary School takes a pro-active approach to help pupils to understand, assess, manage and avoid the risks associated with ‘online activity’. The school recognises its duty of care to its pupils who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

There are a number of definitions of ‘sexting’ but for the purposes of this policy sexting is simply defined as:

- Images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature or are indecent.
- These images are shared between young people and/or adults via a mobile phone, handheld device, computer, ‘tablet’ or website with people they may not even know.

When searching a mobile device the following conditions should apply:

- The search is conducted by the Head Teacher or a person authorised by them and one other person
- A member of the safeguarding team should normally be present
- The search should normally be conducted by a member of the same gender as the person being searched.
- However if the image being searched for is likely to be of a different gender to the person ‘in possession’ then the device should only be viewed by a member of the same gender as the person whose image it is.
- If any illegal images of a young person are found the Safeguarding Team will discuss this with the Police.



## **M: The Prevent Duty**

Schools have a vital role to play in equipping children and young people **to stay safe online, both in and outside school** and also in protecting pupils from the risks of **extremism and radicalisation**. Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on specified authorities, (including schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism (the Prevent Duty).

Terrorist organisations, such as ISIS, are attempting to radicalise and recruit young people through extensive use of social media and the internet. As with any other online risks of harm, every adult in school (teachers and teaching assistants in particular) must be aware of the risks posed by the online activity of extremist and terrorist groups.

The Government has issued statutory guidance in relation to the Prevent Duty (June 2015). In addition, to assist schools and to help recipients understand the implications of the duty, the DfE has also produced non statutory advice (June 2015). Adults should familiarise themselves with the guidance and the advice. This is completed annually during Safeguarding training.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. The school will ensure that suitable filtering is in place. Internet safety is integral to the school's ICT curriculum and the school will ensure it is embedded in the school curriculum.

Keeping children safe from risks posed by terrorist exploitation of social media should be approached by adults in school in the **same way as safeguarding children from any other form of online abuse**.

For the avoidance of doubt, if any adult working in school has a concern that a particular pupil or group of pupils is at risk of radicalisation or terrorist exploitation, through social media or otherwise, they must immediately contact the Head teacher and follow the school's normal safeguarding procedures, including discussing the matter with the school's designated safeguarding lead and where deemed necessary, with children's social care at the Local Authority and the local police.

## **N: Personal use of social media by parents and carers**

14.1 The school encourages all members of the community in the same responsible and respectful use of social media that is taught to pupils. All matters regarding the school are to be communicated via appropriate channels (see complaints procedure) so that they may be dealt with fairly and effectively for all concerned. Abusive, libellous or defamatory comments on social media regarding the school, staff or pupils will be reported to the site's 'report abuse' section for immediate removal.

## **O. Complaints Procedure**

15.1 If a parent/carer or member of staff has any concerns or complaints with regard to social media, they can speak to a member of the SLT, who will investigate the complaint and if necessary will be able to advise on formal procedures for complaint.

## **P. Breaches of Policy and Other Issues**

Any breach of this policy and the duties, responsibilities, professional standards and legal obligations referred to will be regarded as a serious matter and action including disciplinary action in appropriate circumstances will be taken by the Head teacher (or the Governing Body). In serious cases involving employees, this may lead to dismissal without notice on the grounds of gross misconduct.

Where there has been a breach of this policy, the school will also take whatever action is considered appropriate in order to protect the reputation and integrity of the school and the wider school community.

Adults must be aware that any breach of this policy involving a breach of the laws, professional codes or other statutory provisions referred to in this policy may result in legal or other action being taken against them by a body or person other than the school.

The school will regularly remind pupils that signing up to certain social media platforms is not permitted under the age of 13. When the school becomes aware that a child is using a 13+ social media platform, parents will be informed and the expectation will be that parents close the account down. If the school is concerned that a child is exposed to risk online, and that parents are aware of this, the matter may be raised with social services as per the school's child protection procedures.

### **Q: Associated Reading**

The 2018 Keeping Children Safe in Education statutory guidance

Advice for practitioners (including school staff) provides detailed information as to what to do if there are concerns a child is being abused, by the Department of Education, UK Government: <https://www.gov.uk/government/publications/what-to-do-if-youre-worried-a-child-is-being-abused>

Sexting Guidance document by the UK CEOP, the Child Exploitation Command of the National Crime Agency (NCA). This document includes a Sexting response flowchart in Annex 1: <https://www.thinkuknow.co.uk/Teachers/blog/Dates/2013/3/Sexting-in-schools-What-to-do-and-how-tohandle-it>

Appropriate filtering and monitoring guides for schools and education settings, by the UK Safer Internet Centre: <http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriatefiltering-and-monitoring>

CEOP Safety Centre - for help, advice or to report an incident: <http://www.ceop.police.uk/>

The Professionals Online Safety Helpline, by the UK Safer Internet Centre: <http://www.saferinternet.org.uk/about/helpline>

CEOP offers one day training for professionals (paid Ambassador training) on online safety. <https://www.thinkuknow.co.uk/teachers/training/paidtrainingDetails/>

UK Safer Internet Centre advice and resources for teachers and professionals: <http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals>

Online Safety Briefings from young people: [www.onlinesafetylive.com](http://www.onlinesafetylive.com)

Childnet's Professional resources: <http://www.childnet.com/teachers-and-professionals>

Keeping Children Safe Online by the children's charity NSPCC and CEOP, is an online introductory safeguarding course for anyone who works with children: <https://www.nspcc.org.uk/what-you-can-do/get-experttraining/keeping-children-safe-online-course/>

### Part 3:

#### Pupils' agreement and rules for using the Internet at Smithy Street and at home

I understand that these rules are to keep everyone safe and help us use the Internet sensibly and appropriately at school.

- I will ask permission before using the Internet, and only use it when a teacher or another adult is with me.
- I will not look at or delete other people's files.
- I will not bring software or USB flash drives into school without permission.
- I will not download anything from the Internet onto a school computer, unless a teacher tells me to do so
- I will only use the Internet for school work, and follow the instructions given to me by my teacher.
- I will only use my school e-mail when a teacher gives permission.
- The messages I send using my school e-mail account and my blog/ discussion forum posts will be polite and sensible following the school values, as I understand that I am representing my school.
- I will not take part in cyber-bullying and I will not use my personal social media accounts for sending inappropriate or unkind messages to other Smithy Street pupils, their relatives, or staff.
- I will not use a personal e-mail account like Hotmail at school.
- I will never give out my personal details, home address or phone number either by e-mail or on a website
- I will not use Social Media at school unless it is part of a lesson and planned for and supervised by my teacher or another adult.
- If see anything on the Internet that I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files and the Internet sites I visit, to keep me safe.
- I understand that if I deliberately break these rules, I may not be allowed to use the school Internet or computers and Ipads.
- I will not access YouTube or other video content without permission from my class teacher.
- I am aware that I need to be 13 years old to access nearly all social media platforms, including Snapchat, Facebook, Instagram, WhatsApp etc. I know that my teacher may need to speak to my parents if they become aware I am using social media unsuitable for my age
- I will look after the ICT equipment (headphones, keyboard, mouse etc) and leave the computer ready for the next user.

<b>Name</b>	<b>Year Group</b>	<b>Teacher</b>
<b>Signed</b>		<b>Date</b>

## Letter to parents: Using the internet at Smithy Street and at home

### Dear Parents

#### Using the Internet at Smithy Street Primary School and at home

At Smithy Street Primary School we believe that the Internet is an essential part of your child's learning. It offers a huge range of useful and educational material and information and it is becoming an important part of teaching and learning across the curriculum.

Our school provided Internet access to pupils, and we have clear rules and guidelines on how this access will be managed and made as safe as possible

We have taken positive steps to deal with the risk of pupils coming across unsuitable material when they are using the Internet at school:

- We use the LEA approved Internet provider, and there is a filtering system in place restricts access to inappropriate materials.
- We have a comprehensive Internet Use/ E-safety policy for all pupils and school staff.

A copy of the school Internet Use/ E-safety policy is available from our school website

Please would you read the attached Internet Use Agreement that your child has been asked to sign so that you are aware of the rules and guidelines that our school has in place.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

We understand that you may have concerns about how your child uses the Internet at home, and we can provide you with a range of resources and information on how to help your child keep safe on the Internet. There is a selection of links to such resources available for children and parents to see on the school website [www.smithystreet.org.uk](http://www.smithystreet.org.uk) in the section 'pupils- games sites'

It is advisable that Internet access for children at home should normally happen in communal spaces such as the living room or kitchen, instead of the bedroom.

Please ensure that you are always aware what your child is accessing online at home, and supervise your child closely at all times.

Please be aware that due to inappropriate content and on-line safety risks, children need to be 13 years old to access nearly all social media platforms, including YouTube, Snapchat, Facebook, Instagram, WhatsApp etc.

We will let you know if we become aware that your child is accessing such social media at home, and will ask you to ensure that such social media accounts are closed down, as they represent a safeguarding risk.

Should you wish to discuss any aspect of Internet use at Smithy Street School please contact the school for further information

Yours sincerely,

Edith Philipsen  
Headteacher Smithy Street Primary School

## **Staff agreement for Internet use at Smithy Street, Social Media conduct and Data Protection**

***Please refer to the following policies for more detailed information: Internet Acceptable Use/ E-Safety, and Social Media policy, Data Protection policy***

### **Access**

- I will obtain the appropriate log on details and passwords from the ICT Co-ordinator.
- I will not reveal my password(s) to anyone other than the appropriate staff managing the system.
- If my password is compromised, I will ensure I change it.
- I will not use anyone else's password if they reveal it to me.
- I will not allow unauthorised individuals to access school ICT systems or resources.

### **Appropriate Use**

- I will only use the school's digital technology resources and systems, including telephones, text messages and emails for professional purposes, including:
  - contacting parents
  - enabling pupils to communicate with each other,
  - other 'reasonable' usages, as deemed by the Head and Governing Body.
- I will only use the official school website for communicating with parents
- I will never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
- I will not download, use or upload any material which is copyright protected, does not have the appropriate licensing or that might compromise the network.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to a member of the SLT.
- I will ensure that files from personal USB drives, attachments and computers outside the school are virus free before they are opened on the school network

### **Professional Conduct**

- I will not engage in any online activity that may compromise my professional responsibilities or that are in breach of the Teachers' Standards.
- I will ensure that my social media accounts have appropriate privacy settings
- I will never include or 'follow' pupils, former pupils or their families as part of a non-school related social network or group, unless they are related to me (in which case I will disclose this)
- I will never share private information about myself or confidential information about pupils with other pupils or their families
- I will take responsibility for my personal telephones and any personal electronic devices and will keep my personal telephone numbers, login details, passwords, pin details and personal email addresses private and secure.
- In order to safeguard the school's reputation and to avoid harm and distress to staff, pupils and the wider school community:
  - I will ensure that my personal views are not represented in any way as being linked to the school or being the views of the school.
  - I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
  - I will not use social media in any way to attack, insult, criticize, abuse, or defame pupils, family members of pupils, colleagues, the school Governors, the school in general or the wider community.
  - I will never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring them or the school and the wider school community into disrepute or which could be interpreted as reflecting negatively on my professionalism.
- I will not browse, download or send material that could be considered offensive to colleagues.

### **Email**

- I will only use the approved, secure email system for any school business or communication with parents (LGfL Staff Mail).
- I will not communicate with pupils by email unless using approved school email accounts as part of approved school work.

### **Photographs and Video**

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will never associate pupil names or personal information with images or videos published on school social media
- I will never publish photographs, videos or any other types of images of pupils, their families or staff members (without consent), where the school can be identified on personal social media

### **Personal Use**

- I understand that I may use Internet facilities for personal use at lunchtimes, break times and before and after school, where computers are not being used for educational purposes.
- I will not use the school Internet facilities for personal access to social media such as Facebook, Twitter, public discussion groups or bulletin boards, chat rooms or Instant Messaging.
- I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.

### **Teaching and Learning**

- I will always actively supervise, or arrange for suitable adult supervision of pupils that I have directed or allowed to use the Internet.
- I will embed the school's E-Safety curriculum into my teaching, using suitable resources and materials.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I will only use the Internet for professional purposes when pupils are present.

### **Data protection** (for more information please refer to the staff handbook page 27 or the Data Protection policy)

- I will not give out or share personal addresses (including email), telephone numbers of any adult or students (including myself) working at the school, without permission from the Headteacher.
- I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption or send by secure email and that I follow school data security protocols when using any such data at any location.
- I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission.
- I will ensure that computers at home, which are used for work on files containing sensitive and personal information about pupils or staff are password protected and can only be accessed by me.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that we are required by law to disclose such information to an appropriate authority.

### **Concerns**

- I understand that all concerns about communications, social contact or social media/social networking issues must be raised with the Head teacher or a member of SLT immediately.