Online Safety Policy

Adoption by Governing Body

…… (Signature of Chair of Governors)

……November 2018……. (Date)

To Be Revised ……November 2019……..(Date)

Squirrels Heath Junior School
Online-Safety Policy

Contents

1. Introduction and Overview

Rationale:

The purpose of this policy is to:

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

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

Content:

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

Contact:

- Grooming
- Online-bullying in all forms
- Social or commercial theft (including 'frape' (hacking facebook profiles)) and sharing passwords

Conduct:

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

Scope:

This policy applies to all members of Squirrels Heath Junior School community (including staff, students / pupils, volunteers, parents / carers, visitors, governors, community users) who have access to and are users of school computing systems, both in and out of Squirrels Heath Junior School.

Roles and Responsibilities

Role	Key Responsibilities
Head teacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a "safeguarding" culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data and data security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident. • Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of online safety arrangements • To ensure school website includes relevant information

Designated Child Protection Lead	• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
	• Promotes an awareness and commitment to online safety throughout the school community
	• Ensures that online safety education is embedded across the curriculum
	• Liaises with school Computing technical staff
	• To communicate regularly to the designated Safeguarding Governor to discuss current issues
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
	• To ensure that an online safety incident log is kept up to date
	• Facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • online-bullying and use of social media

Role	Key Responsibilities
Governors /Safeguarding governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the Online Safety Governor will include regular review with the Designated Safeguarding Officer
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/ technician	• To report any online safety related issues that arise to the Designated Safeguarding Lead. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • That he / she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of the network / Virtual Learning Environment LGfL / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher for investigation • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures
Office Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are

Role	Key Responsibilities
	fully aware of legal issues relating to electronic content such as copyright laws
All staff and volunteers	• To read, understand and help promote the school's online safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • At the end of the period of employment to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on online-bullying. • To understand the importance of adopting safe online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home

Role	Key Responsibilities
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their children • To consult with the school if they have any concerns about their children's use of technology • To support the school in promoting online safety and endorse pupils' use of the Internet and the school's use of photographic and video images
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology

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

- Policy to be posted on the school website and emailed to all staff
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in the school office

Handling complaints:

- The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions.
- The Designated Safeguarding Lead acts as first point of contact for any complaint. Infrigements must be reported on the same day.
- Any concerns about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority Designated Officer).

Handling a sexting incident:
UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
    - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?

- Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of imagery?
- What is the impact on the pupils involved?
- Do the pupils involved have additional vulnerabilities?
- Does the young person understand consent?
- Has the young person taken part in this kind of activity before?

If a referral should be made to the police and/or children's social care

- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Review and Monitoring:

The Online Safety policy is referenced from within other school policies: Safeguarding policy, Behaviour policy and Staff Handbook.

- The school has a Designated Safeguarding Lead who will be responsible for document ownership, review and updates.

- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online Safety policy is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders. All amendments to the school online safety policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil Online Safety curriculum:
Squirrels Heath Junior School

- Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To STOP and THINK before they CLICK
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - To know how to narrow down or refine a search;
    - To understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - To understand acceptable behaviour when using an online environment / email, i.e. Be polite, do not use abusive language, keep personal information private;
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned on privacy settings;
    - To understand why they must not post pictures or videos of others without their permission;
    - To know not to download any files – such as music files - without permission;
    - To have strategies for dealing with receipt of inappropriate materials;
    - To understand why and how some people will 'groom' young people for sexual reasons;
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. Parent or carer, teacher or trusted staff member, or an organisation such as Child Line.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an Acceptable Use Agreement which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling.

Staff and governor training:
Squirrels Heath Junior School
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education program.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety policy and the school's Acceptable Use Policies.

Parent awareness and training:
Squirrels Heath Junior School
- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site;
    - Demonstrations, practical sessions held at school;
    - Suggestions for safe Internet use at home;
    - Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct:
At Squirrels Heath Junior School, all users:
- Are responsible for using the school computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and online-bullying.

Staff:
- Are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.
- Know to be vigilant in the supervision of children at all times, as far as is reasonable.
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use and using age appropriate search engines

Students/Pupils:
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers:

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management:

At Squirrels Heath Junior School:

- There is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. The Local Authority and UK Safer Internet Centre helpline) in dealing with online safety issues.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- We will immediately refer any suspected illegal material to the appropriate authorities.

Social Media - Protecting Identity

At Squirrels Heath Junior School we understand the need to protect personal information. We will do this by:

- Ensuring that personal data is not published
- Providing appropriate training for staff
- Ensuring that there is clear guidance so that responsibilities, procedures and sanctions are clear

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Dealing with unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be unlawful/inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	

Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gambling				X	

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering:**

Squirrels Heath Junior School:

- Has the educational filtered secure broadband connectivity through LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment / LGfL secure platforms such as J2Bloggy, etc.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Computing coordinator. Our system administrator logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;

- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup):**

Squirrels Heath Junior School

- Uses individual, audited log-ins for all users - the London USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Storage of all data within the school will conform to the UK data protection requirements;
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, Squirrels Heath Junior School:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide *a* different username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. They are also expected to use a personal password;
- All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform and their own school approved email account;
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 60 minutes and have to re-enter their username and password to re-enter the network.];
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes it clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and

that they notify the school of any “significant personal use” as defined by HM Revenue & Customs.

- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school’s network resources from remote locations by staff is restricted and access is only through school / RM Portico;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides staff with access to content and resources through the approved Learning Platform which staff access using their username and password (their school network username and password);
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit’s requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school Computing systems regularly with regard to health and safety and security.

Password policy:

- Squirrels Heath Junior School makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.

E-mail:

Squirrels Heath Junior School

- Provides staff with an email account for their professional use, LGfL Staffmail and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@shj.havering.sch.uk / head@lgflmail.orguk / or class e-mail addresses (with one or more staff having access to an aliased/ shared mailbox for a class) for communication with the wider public;

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up to date;
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police;
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

Pupils:

- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules;
- Pupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection;
- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work;
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this;
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the LGfL e-mail systems on the school system;
- Staff only use LGfL e-mail systems for professional purposes;
- Access in school to external personal e-mail accounts may be blocked;
- Never use email to transfer staff or pupil personal data. If there is no secure file transfer solution available, then the data or file must be protected using security encryption.

School website

- The Head teacher, supported by the Governing Body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: administration officer and deputy head teacher;
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address office@shj.havering.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images;
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Cloud Environments

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools LEARNING PLATFORM will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform.

Social networking.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils / parents / carers or school staff;
- They do not engage in online discussion on personal matters relating to members of the school community ;
- Personal opinions should not be attributed to the *school* or local authority;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils are:

- Taught about acceptable behaviours and how to report misuse, intimidation or abuse
- Required to sign and follow our Acceptable Use Agreement

Parents are

- Reminded about social networking risks and the need to supervise pupils
- Reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices:
At Squirrels Heath Junior School:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure all staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record
- We ensure Acceptable Use Agreement forms are signed and adhered to.

.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 60 minutes idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use Portico for remote access into our systems.
- We use LGfL's USO to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We use LGfL's GridStore remote secure back-up / named alternative solution> for disaster recovery on our <network / admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off and handed in at the school gate each morning. They may be collected at the end of the day from the designated member of staff in the playground. Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

.

Digital images and video

In Squirrels Heath Junior School:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendix A1

Acceptable Use Agreement: All Staff, Volunteers and Governors

This acceptable use policy reflects the school on line policy. The school will ensure that staff, volunteers and governors will have good access to computing to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff, volunteers and governors to agree to be responsible users.

The acceptable use policy covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. 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 and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, or any Local Authority (LA) system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business. This is currently: LGfL Staff Mail
- I will only use the approved email system and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the School Business Manager.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network 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 and other computing 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of mobile phones / devices at school and will only use in staff areas.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff-only drive within school.
- I will use the school's Learning Platform in accordance with school protocols.
- 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 ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the LGfL / school approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- 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 I am required by law to disclose such information to an appropriate authority.
- I will alert the Designated Safeguarding Officer if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the designated Child Protection lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to* the Head on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- Staff that have a teaching role only*:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others online safety and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .....Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date.....

Full Name ..... (printed)

Appendix 2

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite 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 give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: Date:

Appendix A3

Online-safety agreement form: Parents

Internet and computing: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter / son access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment
- Computing facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e- behaviour they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.

- In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process: https://www.thinkuknow.co.uk/parents/browser-safety/

Appendix Four

'Prevent Duty' within education settings –

The Department for Education offers advice to coincide with the prevent duty, introduced as part of the Counter-Terrorism and Security Act 2015. From 1st July 2015 organisations including schools must to take steps to prevent people from being drawn into terrorism.

Ofsted's revised common inspection framework for education, skills and early years, which came into effect from 1 September 2015, makes specific reference to the need to have safeguarding arrangements to promote pupils' welfare and prevent radicalisation and extremism. As with managing other safeguarding risks, all staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Schools and childcare providers already play a vital role in keeping children safe from harm, including from the risks of extremism and radicalisation, and in promoting the welfare of children in the care of this school. The prevent duty reinforces existing safeguarding duties in school.

All schools and childcare providers should be aware of the increased risk of online radicalisation, as different organisations seek to radicalise young people through the use of social media and the internet. As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups. The Online safety policy for this school outlines safe appropriate behaviours and how to monitor and support children online, in and away from the school.

General safeguarding principles apply to keeping children safe from the risk of radicalisation as set out in the relevant statutory guidance, **Working together to safeguard children** and **Keeping children safe in education**.

Extremism Risk Indicators

Online activity

- increased time spent online;
- secretive online behaviours;
- becomes obsessive about being online;
- gets angry when he or she can't get online;
- changes screens or turns off computer when an adult enters a room;

Identity

- the student/pupil is distanced from their cultural /religious heritage and experiences;
- discomfort about their place in society;
- personal Crisis – the student/pupil may be experiencing family tensions;
- a sense of isolation;
- low self-esteem;
- they may have dissociated from their existing friendship group and become involved with a new and different group of friends;
- they may be searching for answers to questions about identity, faith and belonging.

Personal Circumstances

- migration;
- local community tensions; and
- events affecting the student/pupil's country or region of origin may contribute to a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy

Unmet Aspirations

- the student/pupil may have perceptions of injustice;
- a feeling of failure;
- rejection of civic life;

Experiences of Criminality

- involvement with criminal groups
- imprisonment; and
- poor resettlement/reintegration on release

Special Educational Needs

- social interaction
- empathy with others
- understanding the consequences of their actions; and awareness of the motivations of others

More critical risk factors could include:

- being in contact with extremist recruiters;
- accessing violent extremist websites, especially those with a social networking element;
- possessing or accessing violent extremist literature;
- using extremist narratives and a global ideology to explain personal disadvantage;
- justifying the use of violence to solve societal issues;
- joining or seeking to join extremist organisations; and
- significant changes to appearance and/or behaviour;
- experiencing a high level of social isolation, resulting in issues of identity crisis and/or personal crisis.

Members of staff must follow the school's normal safeguarding procedures, including reporting to the school's designated safeguarding lead on the day they have a concern. The designated lead with raise with the safeguarding advisor in Havering and where deemed necessary, with Early Help or MASH.

- The Prevent officer in Havering is PC Greig Urquhart, Greig.Urquhart@met.pnn.police.uk Tel: 07766227261
  Workshop to Raise Awareness of Prevent (WRAP) is offered in Havering and has been developed by the Home Office as a core training product for this purpose.

- Anti terrorist hotline 0800 789 321

- The Department for Education has set up a telephone helpline (020 7340 7264) and an email address (counter.extremism@education.gsi.gov.uk) to enable people to raise concerns directly with the department.

- Reporting online extremism http://www.seeitreportit.org/

- To report terrorist content on the web go to https://www.gov.uk/report-terrorism

Working together to prevent terrorism http://www.ltai.info/