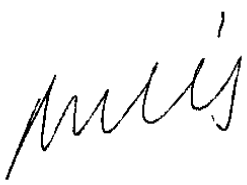
e-Safety Policy

Prepared by:	Beth Tillyer
Agreed by staff:	Spring 2017
Review:	Spring 2018

Signed

Chair of Governors:



Headteacher:

CHASE BRIDGE PRIMARY SCHOOL

Introduction, aims, purpose of policy

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children and adults. The policy highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. This policy is designed to ensure safe internet use by pupils in school, but also while on-line at home etc.

The policy sets out the key principles expected of all members of the school community at Chase Bridge with respect to the use of ICT based technologies. It documents the management of the ICT infrastructure and network.

Please also refer to the following policies and documents

- Data Protection Policy
- Safeguarding Policy
- Behaviour and Anti-Bullying Policy
- Freedom of Information Act
- Complaints Policy

Contents

Role of the Headteacher
The Headteacher:
- Takes overall responsibility for the e-safety provision
- Ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- Is responsible for ensuring staff receive suitable training in their e-safety roles
- Is aware of procedures to be followed in the event of a serious e-safety incident

Role of the E-safety Co-ordinator
The E-safety co-ordinator:
- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy
- Promotes an awareness and commitment to e-safeguarding throughout the school community
- Ensures that e-safety education is embedded across the curriculum
- Liaises with school ICT technical staff
- To ensure that an e-safety incident log is kept up to date
- Communicates regularly with SLT and the designated e-safety Governor to discuss current issues, review incident logs
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident

Role of the Governors
The Governors:
- Ensure that the school follows all current e-safety advice to keep the children and staff safe
- Review the effectiveness of the policy. Support the school in encouraging parents and the wider community to become engaged in e-safety activities
- The role of the E-Safety Governor will include:
    - Termly reviews of the incident logs with the E-Safety Co-ordinator

Staff training
- We provide as part of our induction process, all new staff with information and guidance on the e-safety policy and the school's Acceptable Use Policies.
- Make regular training available to staff on e-safety issues e.g. inset days, staff meetings
- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection

Expected conduct
In this school, all users:
- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Policy which they will be expected to sign before being given access to school systems (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- 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 e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

- 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 on cyber-bullying

Incident Management (See appendix 1)

In this school:

- There is strict monitoring and application of the e-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) in dealing with e-safety issues
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed and reported to the school's senior leaders and the Governors
- Parents / carers are specifically informed of e-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

E-safety curriculum

Chase Bridge has a clear, progressive e-safety education programme as part of the Computing curriculum/PSHE curriculum. It is built on LA / LGfL e-safeguarding and e-literacy framework for EYFS to Y6/ national guidance. 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;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- 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 understand the importance of using websites and apps that are age appropriate;
- to have strategies for dealing with receipt of inappropriate materials;

- [for older pupils] 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 ChildLine or the CLICK CEOP button.
- Computing lessons are age-appropriate and supports the learning objectives for specific curriculum areas.
- 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;
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.

Managing the ICT infrastructure
Internet access, security (virus protection) and filtering

- We have an educational filtered secure broadband connectivity
- We use a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Chase Bridge uses whole school level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- We use Sophos anti-virus software etc. and network set-up so pupils cannot download executable files;
- We use 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;
- We only unblock external social networking sites for specific educational or school purposes
- We work in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- We are vigilant in our supervision of pupils' use at all times, as far as is reasonable, and use common-sense strategies in learning resource areas where older pupils have more flexible access;
- We are vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Chase Bridge informs staff and students that that they must report any failure of the filtering systems directly to the IT Teaching Assistant. The IT Teaching Assistant logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- We provide advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents;
- We immediately refer any material we suspect is illegal to the appropriate authorities – Police and the LA.

Network management (user access, backup)

Chase Bridge:

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- 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, Chase Bridge:

- Ensures staff read and sign that they have understood the school's e-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. 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. From Year 3 they are also expected to use a personal password;
- 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;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day. The school Premises Team will conduct end of day checks to ensure that all IT equipment has been shut down.
- 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 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.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- 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 / LA approved systems: *e.g. staff access their area through the RDP Gateway system*
- 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 pupils and staff with access to content and resources through approved Learning Platforms which staff and pupils access using their username and password (their USO 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;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

All staff have their own unique username and private password to access school systems. Passwords should be strong and kept private. Different systems will use different usernames and passwords and users are prompted to change passwords on a regular basis.

E-mail

Staff:

- Staff are provided with an email account for their professional use
- Access in school to external personal e mail accounts may be blocked
- The school 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@chasebridge.richmond.sch.uk
- We 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.
- 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.

Pupils:

- We use LGfL LondonMail with Upper KS2 pupils and lock this down where appropriate using LGfL SafeMail rulesPupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.
- Upper KS2 Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- 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.

School website

- The Headteacher 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.
- 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, e.g. info@chasebridge.richmond.sch.uk.
- 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 geo data in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Learning platforms

- Uploading of information on the schools' learning platforms 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 secure network directories will only be accessible by staff members
- In school, pupils are only able to upload and publish within school approved and closed systems

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

Data security: Management Information System access and Data transfer
Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- We ensure 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 by the School Business Manager.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form.
  - staff,
  - governors,
  - pupils
  - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platforms access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to lock their computer if they are leaving it unattended.
- 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 RDP with its 2-factor authentication for remote access into our systems.
- We use LGfL's USO FX 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 a secure online back up service which complies to the UK Data Protection requirements
- Paper based sensitive information is collected by secure data disposal service.

Equipment and Digital Content

Personal Devices

Staff are not permitted to use personal devices to transfer or store sensitive data using non-school approved email accounts or any cloud based services. When working off-site staff will use a 2-factor authentication to remote access onto the schools network systems.

All school personnel are trained to:

- be discreet and confidential;
- consider the safe and secure positioning of computers;
- turn off computers when not in use;
- remember password access;
- lock filing cabinets and doors to offices;
- shred confidential material;
- clear their desk before they leave school

Personal mobile phones and mobile devices

The use of personal mobile technology is prohibited when staff or visitors are responsible for children's safety and well-being. There are strictly limited exceptions to this, for example when the technology protects or keeps the children safe; when there is direct relevance to a lesson; when used as part of official school communications.

- Mobile phones brought into school are entirely at the staff member 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.
- All visitors are requested to keep their phones on silent.
- 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.
- 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.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- 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.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils unless as part of an approved and directed curriculum-based activity
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We operate an 'opt out' permission policy 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 with their full names in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- 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.

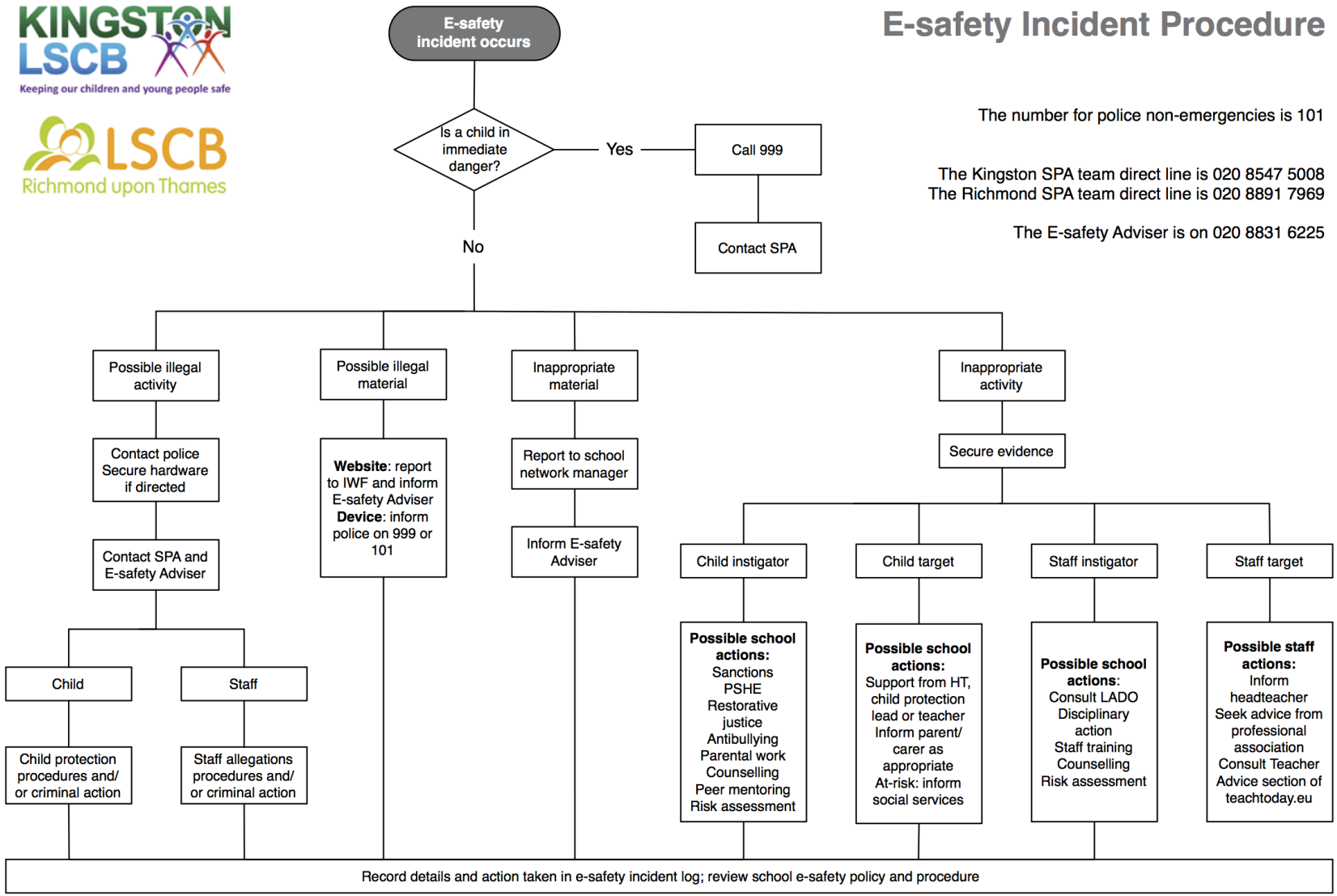
Asset disposal

- 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.

Handling complaints:

- The school will take all reasonable precautions to ensure e-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. Sanctions available include:
    - interview by class teacher, Head of Year or Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period
    - referral to LA / Police.
- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Appendices


KINGSTON LSCB
Keeping our children and young people safe
LSCB
Richmond upon Thames
E-safety incident occurs
E-safety Incident Procedure
Is a child in immediate danger?
Yes
Call 999
Contact SPA
No
The number for police non-emergencies is 101
The Kingston SPA team direct line is 020 8547 5008
The Richmond SPA team direct line is 020 8891 7969
The E-safety Adviser is on 020 8831 6225
Possible illegal activity
Contact police Secure hardware if directed
Contact SPA and E-safety Adviser
Child
Staff
Child protection procedures and/ or criminal action
Staff allegations procedures and/ or criminal action
Possible illegal material
Website: report to IWF and inform E-safety Adviser Device: inform police on 999 or 101
Inappropriate material
Report to school network manager
Inform E-safety Adviser
Inappropriate activity
Secure evidence
Child instigator
Child target
Staff instigator
Staff target
Possible school actions: Sanctions PSHE Restorative justice Antibullying Parental work Counselling Peer mentoring Risk assessment
Possible school actions: Support from HT, child protection lead or teacher Inform parent/ carer as appropriate At-risk: inform social services
Possible school actions: Consult LADO Disciplinary action Staff training Counselling Risk assessment
Possible staff actions: Inform headteacher Seek advice from professional association Consult Teacher Advice section of teachtoday.eu
Record details and action taken in e-safety incident log; review school e-safety policy and procedure