ST. ANDREW'S CE PRIMARY SCHOOL
E-SAFETY POLICY

1. Introduction and Overview

At St. Andrew's we welcome you to our happy, safe and Christian family, where we encourage everyone to do their very best. Our vision is to inspire our children to be confident individuals, who are excited about learning and curious about the world that they live in.

These principles also apply to the 'virtual' or digital world as to the school's physical buildings. We recognise that e-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology. Our e-Safety Policy incorporates current guidance from the Department for Education (DfE) and the Londong Grid for Learning (LGfL). It has been agreed by the staff and approved by governors. It will be reviewed annually.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St Andrew's CE Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of St Andrew's CE Primary 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:

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data
- Extremism

Roles and Responsibilities

The Executive Headteacher (Jayne Mitchell)

- To be responsible for e-Safety provision
- To be responsible for data and data security (SIRO)
- To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL
- To be responsible for ensuring that staff receive suitable training to carry out their e-Safety roles and to train other colleagues, as relevant
- To be aware of procedures to be followed in the event of a serious e-safety incident.
- To receive regular monitoring reports from the e-Safety Co-ordinator
- To ensure that there is a system in place to monitor and support staff who carry out internal e-Safety procedures (eg. Network manager)

Roles and Responsibilities (continued)

E Safety Co-ordinator (Heather Coward)

- To take day to day responsibility for e-Safety issues and have a leading role in establishing and reviewing the school e-Safety policies/documents
- To promote an awareness and commitment to e-Safety safeguarding throughout the school community
- To ensure that e-Safety education is embedded across the curriculum
- To liaise with school Computing technical staff
- To communicate regularly with SLT and Governors to discuss current issues, review incident logs and filtering/change control logs
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
- To ensure that an e-Safety incident log is kept up to date
- To facilitate training and advice for all staff
- To liaise with the Local Authority and relevant agencies
- To be aware of current e-safety issues and legislation, and be aware of the potential for serious child protection issues

Governors

- To understand e-Safety issues and strategies at this school.
- To keep up to date with local and national guidance on e-Safety
- To update and review policy documents on an annual basis.

Computing Curriculum Leader (Lucy Chambers-Harding)

- To oversee the delivery of the e-Safety element of the Computing curriculum
- To liaise with the e-Safety coordinator regularly

Network Manager/technician (Peter Gray)

- To report any e-Safety related issues to the e-Safety coordinator.
- 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's IT system
- The ensure that the school's policy on web filtering is applied and updated on a regular basis
- To inform LGfL of issues relating to the filtering applied by the Grid
- That he keeps up to date with the school's e-safety policy and technical information in order to effectively carry out his online safety role and to inform and update others as relevant
- That the use of the network, remote access , email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-safety Co-ordinator for action
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Data Manager (Vivienne Adedze)

- To ensure that all data held on pupils on the school office machines have appropriate access controls in place

Teachers

- To embed e-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 fully aware of legal issues relating to electronic content such as copyright laws

Roles and Responsibilities (continued)

All staff

- To read, understand and help promote the school's e-Safety policies and guidance
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy
- To be aware of e-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 e-Safety coordinator
- To maintain an awareness of current e-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.

Pupils

- Read, understand, sign and adhere to the Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- 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.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good online 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
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home

Parents/Carers

- To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children at admissions
- To access the school website, social media pages and pupil records in accordance with the relevant school Acceptable Use Agreement.
- To consult with the school if they have any concerns about their children's use of technology

External groups

- Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication:

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

- Policy to be posted on the school website
- Policy to be part of school induction 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 pupil and personnel files.

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. Sanctions available include:
    - Interview/counselling by e-Safety Coordinator / Exective Headteacher; / member of SLT
    - 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 Exective Headteacher.
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school's child protection procedures.

Review and Monitoring

The Online safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- St Andrew's has an e-Safety coordinator who will be responsible for document ownership, review and updates.
- The e-Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-Safety policy has been written by the school e-Safety Coordinator and 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 the Governors. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Curriculum Content and Planning

Designated lessons on e-Safety are taught during the academic year and staff will remind children of different aspects of e-Safety as they use the internet throughout the year. Safer Internet Day is celebrated each February. Teachers use CEOP's (The Child Exploitation and Online Protection Centre) 'Think you know' website, which provides different resources for all staff to use to support the teaching and learning of E-Safety, providing different activities for children to work through. These sessions will empower and protect children both online and off. Creative Curriculum and Cross Curricular Links Internet use will enhance learning.

At St Andrew's:

- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines and objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- When appropriate the school will use 'safer' search engines with pupils such as http://yahooligans.yahoo.com/ | http://www.askforkids.com/ and activates 'safe' search where appropriate. The school is vigilant when conducting 'raw' image search with pupils e.g. Google search.
- We foster a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- We ensure pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or e-safety co-ordinator
- Pupils are taught how to evaluate Internet content and to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- We ensure pupils and staff know what to do if a cyber-bullying or other e-safety incident occurs.

Staff and Governor Training

At St Andrew's we:

- 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;
- Make regular training available to staff on online safety issues and the school's online safety education program;
- Provide, as part of the induction process, all new staff (including voluntary staff)with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent Awareness and Training

At St Andrew's we run 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.
- Sessions run by Lambeth Safeguarding Team

3. Incident management

At St Andrew's:

- There is strict monitoring and application of the e-Safety safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply 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 regional broadband grid, 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 e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- 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

4. Managing the IT and Computing infrastructure

Internet access, security (virus protection) and filtering

At St Andrew's:

- We operate the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- We use 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;
- We ensure our network is healthy through the use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and 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 block all Chat rooms and social networking sites except those that are part of an educational network;
- We only unblock other external social networking sites for specific purposes / Internet Literacy lessons;
- We work in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;

Internet access, security (virus protection) and filtering (continued)

- We are vigilant in our supervision of pupils' use at all times, as far as is reasonable, and we use common-sense strategies in learning resource areas where older pupils have more flexible access;
- We ensure all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- We ensure pupils only publish within an appropriately secure environment: the school blog and LGfL secure platforms such as J2Bloggy, etc.
- We require staff to preview websites before use [where not previously viewed or cached]. We plan 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 , …..
- We never allow a 'raw' image search with pupils e.g. Google image search;
- We inform all users that Internet use is monitored;
- We inform staff and pupils that that they must report any failure of the filtering systems directly to the e-Safety co-ordinator. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- We make 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;
- 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 – the Police and the Local Authority.

Network management (user access, backup)

At St Andrew's;

- We use individual, audited log-ins for all users - the London USO system;
- We ensure 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.
- We ensure 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.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- The network is set up 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;
- 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;
- 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.
- It is 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.
- We maintain equipment to ensure Health and Safety is followed e.g. equipment installed and checked by approved Suppliers / LA electrical engineers
- We have 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. SEND coordinator - SEND data;
- We ensure that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems.
- We do 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 and parents using a secure portal to access information on their child;
- Pupils and staff are provided with access to LGfL content and resources which staff and pupils access using their username and password (their USO username and password);
- There are clear responsibilities for the daily back up of MIS and finance systems and other important files;

Network management (continued)

- Clear disaster recovery system are in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- We use the DfE secure s2s website for all CTF files sent to other schools;
- We ensure 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);
- We follow 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;
- The school IT systems are reviewed regularly with regard to health and safety and security.

E-mail

At St Andrew's we;

- Provide staff with an LGfL email account for their professional use, and makes it clear that personal email should be through a separate account;
- Know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.
- Do 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@schoolname.la.sch.uk / head@schoolname.la.sch.uk / 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 ensure that email accounts are maintained and up to date
- Never use email to transfer staff or pupil personal data. We use Egress Switch, an LA / approved system.
- Provide highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils and Londonmail for older pupils. Pupils are introduced to, and use e-mail as part of the IT/Computing scheme of work.
- Teach pupils about the online safety and 'netiquette' of using e-mail both in school and at home
- 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.
- Report messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Know 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.

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. Information or individual e-mail identities will not be published;
- Photographs of children 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.

Social networking

School staff will ensure that in private use:

- No reference should be made in social media to 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.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice.
- We do not reveal any such recordings outside of the staff and will not use for any other purposes.

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

Strategic and operational practices

At St Andrew's:

- The Executive 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 have listed the information and information asset owners in a spreadsheet.
- 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
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
- 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 and Social Care.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / 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 and network access work within the approved system and follow the security processes required by those systems.

Technical Solutions

- We require staff who have access to sensitive documents to log-out of systems when leaving their computer, but also enforce lock-out after 10 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 a VPN solution 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 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 a lockable storage cabinet..
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use LGfL's GridStore remote secure back-up for disaster recovery on our network server.
- 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 and we are using secure file deletion software.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupils & 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.
- Pupils are able to bring a mobile phone into school if they walk home alone. Pupils and parents read and sign the mobile phone policy. Mobile phones which are brought into school must be turned off and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- If a pupil 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.
- 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 Headteacher.
- 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.

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.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils 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.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

At St Andrew's:

- We gain parental 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/filters 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 IT 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 identity 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.

Approved by: ……

Date: January 2017

Next review date: January 2018

Acceptable Use Agreement: All Staff, Volunteers and Governors Agreement Form

Covers use of all digital technologies in school: i.e. e-mail, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will follow the separate e-safety policy (including mobile and handheld devices).
- 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 e-mail / Internet / intranet / network or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network / information security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the school approved e-mail system(s) for any school business, including communication with parents. This is: *LGfL StaffMail.* I will only enter into communication regarding appropriate school business.
- I will only use the school's approved systems to communicate with pupils, and will only do so for teaching & learning purposes.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to the designated e-Safety Officer.
- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- 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 drives) 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 Sophos anti-virus and other ICT '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 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 school approved system.
- I will follow the school's policy on use of mobile phones / devices at school.
- I will use the school's St Andrew's All Star Blog and Twitter account 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, that 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 follow e-security protocols when accessing school resources remotely (such as from home).
- 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 that is 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 school's child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I will only use any other/LA system I have access to in accordance with its policies.
- I understand that 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 a senior member of staff / named child protection officer at the school.
- I understand that all Internet usage and network usage can be logged, and that this information can be made available to the Head / Safeguarding Lead on their request.
- *Staff that have a teaching role only:* I will embed the school's e-safety / digital literacy curriculum into my teaching.

Acceptable Use Agreement: All Staff, Volunteers and Governors Agreement Form

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding 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 that I read and understand the school's most recent e-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: Headteacher

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

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

Full Name ..... (printed)