E-SAFETY POLICY

ST ANN'S SCHOOL

RIGHTS RESPECTING SCHOOLS
unicef UNITED KINGDOM
LEVEL 2

E-SAFETY POLICY ST ANN'S SCHOOL

based on LGFL School E-Safety Policy Template 2015

St Ann's is a county maintained special school for young people aged 11 to 19 years with complex profound to severe learning difficulties including those on the Autistic Spectrum Continuum. The great majority of students are assessed as functioning between P1 and P5 equivalent to a chronological age of between 3 months and 3 years. St Ann's is a Unicef Rights Respecting School (Level 1) and as demonstrated through our daily practice, is absolutely committed to promoting all aspects of the United Nations Charter on the Rights of the Child both locally and internationally. Articles 3 (best interests of the child), 17 (access to information from mass media) 34 (sexual exploitation) and 36 (other forms of exploitation) are particularly pertinent to this E-safety policy.
The school and Governing Body in consultation with the Local Authority Educational Consultant ICT, decided to adopt the LGFL School E-Safety Policy Template, with very few amendments, for the following reasons :

- It is broad ranging and written by experts within the field
- It is regularly updated in order to reflect fast changing technologies and any new legislative requirements
- Our young people live in a technologically driven society and whilst exposed to some of the inherent risks, they also derive enormous benefit from doing so.
- IT is an area where some of St Ann's students excel. Like their mainstream peers they work intuitively by trial and error. On occasion this process may expose them to inappropriate material, particularly as for some students using a PC or tablet is one of the few areas where they successfully demonstrate self occupancy skills for short periods of time.

Bearing the above in mind there may be aspects of this policy which may only be relevant to one or two students because of the impact of their severe cognitive impairment. However it is the duty of all adults to safeguard the interests of all children and young people (Refer to St Ann's Child Protection Policy) and therefore it is an absolute requirement that all adults, who work with or come into contact with St Ann's students, strictly adhere to all directives as stated within this E safety policy.

Contents

- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the ICT Infrastructure
    - Internet access, security (virus protection) and filtering
    - Network management (user access, backup, curriculum and admin)
    - Passwords policy
    - E-mail
    - School website
    - Learning platform/restricted area of website
    - Social networking
    - Video Conferencing

5. Data Security
    - Management Information System access
    - Data transfer

6. Equipment and Digital Content
    - Personal mobile phones and devices
    - Digital images and video
    - Asset disposal

Appendices:

1. Acceptable Use Agreement (Staff)
2. Protocol for responding to e-safety incidents
   http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements
   http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards
3. Protocol for Data Security
4. Search and Confiscation guidance from DfE
   https://www.gov.uk/government/publications/searching-screening-and-confiscation

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 St Ann's School with respect to the use of ICT-based technologies.
- safeguard and protect the students and staff of St Ann's School.
- assist school staff working with students 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 cyberbullying 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 violence and online pornography, ignoring age ratings in games (exposure to violence associated with often racist language)
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- 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)

(Ref Ofsted 2013)

Scope (from SWGfL)
This policy applies to all members of St Ann's School community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St Ann's School.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the *school* site and empowers members of staff to impose disciplinary penalties for

inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school . The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility 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

E-Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• 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 communicate regularly with SLT and the designated e-safety Governor 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
	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• Is regularly updated in e-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
	  • cyber-bullying and use of social media

Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To 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:

	• regular review with the E-Safety Co-ordinator including e-safety incident logs, filtering / change control logs.
Curriculum Manager (DHT)	● To oversee the delivery of the e-safety element of ICT within the broader curricular offer eg through Themes and accredited programmes. ● To liaise with the e-safety coordinator regularly
Trusol and ICT technician	● To report any e-safety related issues that arises, to the e-safety coordinator. ● 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 e-safety policy and technical information in order to effectively carry out their e-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 /Headteacher for investigation / action / sanction* ● 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 e-security and technical procedures
School Business 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 e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
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 (St Ann's Policy for Photos and Use of Videos currently being developed) • 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 students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Students	• To learn about keeping safe (as appropriate to the individual's developmental level) with respect to e-safety through a broad range of curricular opportunities • Commensurate with each individual's cognitive ability to use technology in a responsible manner • Commensurate with each individual's cognitive ability to seek help from a trusted adult if he/she feels upset, worried or vulnerable when using online technology • Commensurate with each individual's cognitive ability to help the school in the creation/ review of e-safety policies
Parents/carers	• to support the school in promoting e-safety eg through attending e-safety coffee mornings and training sessions • to consult with the school if they have any concerns about their young person'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/students/community in the following ways:

- Policy to be posted on the school website, intranet and staff room
- Policy to be part of school induction pack for new staff
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- For students, through a broad range of curricular opportunities, relating to technology, commensurate with each individual's cognitive ability.

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 students are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview with E-Safety Coordinator / 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.

Review and Monitoring
The e-safety policy is referenced from within other school policies: ICT policy, Child Protection policy, Anti-Bullying policy and in the School Impact Plan, Positive Behaviour policy, Personal, Social and Health Education and for Citizenship policies .

- The school 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 is based on the EGFL e-safety policy and has been amended by the teaching staff group, including the Headteacher and e-safety co-ordinator. It is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by teachers, the SLT and approved by Governors and other stakeholders. All amendments to the school e-safeguarding policy will be discussed in detail with parents/carers, governors and all members of school staff.

Version Control

As part of the maintenance involved with ensuring that the e-safety policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	St Ann's School E-Safety Policy
Version	1.3
Date	21.09.15
Author	Teaching staff group including E-safety coordinator and Headteacher
Approved by Head teacher	25.09.15
Approved by Governing Body	30.09.15
Next Review Date	September 2021

Modification History			
Version	Date	Description	Revision Author

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the wider curriculum appropriate to the cognitive ability of students with complex profound to severe learning difficulties.
- Students are encouraged and supported to develop some of the following skills, commensurate with their developmental stage and level of understanding
- St Ann's Student Voice (Student Council) will be actively involved in developing a simple, symbolled, student friendly 'Keep IT Safe' poster.
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy
    - to know how to narrow down or refine a search;
    - 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 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 have strategies for dealing with receipt of inappropriate materials;
    - to have some understanding of how some people will 'groom' young people for sexual reasons;
    - to understand some aspects 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.

- Plans Internet use carefully to ensure that it is commensurate with the student's cognitive ability and supports the learning objectives for specific curriculum areas.

- Will remind students about 'think before you click' and the 'Keep IT Safe' poster.
- 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 to a limited degree and where appropriate students, 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 where appropriate students 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

This 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 e-safety issues and the school's e-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 e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of Acceptable Use Information to new parents/carers, to ensure that principles of e-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

In this school, all users:

- are responsible for using the school ICT 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 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. Refer to St Ann's policy on Photos and Use of Video, currently being developed.

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.
- Teachers and Teaching Assistants need to be aware as to which students have permission to be filmed and photographed. An updated list will be made available at the beginning of each academic year.

Also refer to Roles and Key Responsibilities Table (Pages 5-8 of this document)

Incident Management

In this school:

- there is strict monitoring and application of the e-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 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.
- 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
- St Ann's will ensure that the school is compliant with recently introduced Protect legislation and will guard against students being exposed to internet content which may have a radicalisation remit.

4. Managing the ICT infrastructure

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

This school:

- Has the educational filtered secure broadband connectivity through the 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 health through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and students cannot download executable files; anti-virus software will be periodically checked by ICT technician.
- 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 where staff need to access personal level data off-site;
- Routinely only uses each student's initials and date of birth - when sharing information
- 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 student access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- 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 students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas according to each student's cognitive level.
- Ensures all staff have signed an acceptable use agreement form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school website, as a key way to direct students to age, subject and developmentally appropriate web sites;

- Plans the curriculum context for Internet use to match students" 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 , ….. (A bookmark icon can be added to Chrome)
- 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 e-safety co-ordinator, who will then log or escalate the issue 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 students, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**
  This school
  - Uses individual, audited log-ins for all users;
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
  - Ensures the e-safety co-ordinator/ 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

    Students 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, this school:

- 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 classes with an class network log-in username.
- Makes clear that no one should log on as another user and makes clear that students 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 students and one for staff. Staff and students 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.
- 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 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.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager, equipment installed and checked by approved Suppliers / 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;
- 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:

- 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;
- Provides pupils and staff with access to content and resources through a restricted area of the web site which staff and pupils access using their 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;
- Will use our broadband network for our newly installed CCTV system which is being set up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all student 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 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 ICT systems regularly with regard to health and safety and security.

Password policy

- This 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.
- We require staff to change their passwords into the MIS, LGfL USO admin site, other secure system at least once a year.

E-mail

This school

- Provides staff with an email account for their professional use, Lgflmail and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of students or staff on the school website.
- Will contact the Police if one of our staff or students 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 WebScreen 2 filtering monitors and protects our Internet access to the World Wide Web.

Students

- The great majority of St Ann's students do not have the cognitive ability to create and send emails.
- 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.
- Where appropriate students 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 email, 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.

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

- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX,
- Staff 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. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;
- All staff sign our school Acceptable Use 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.

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 adminmail@st-anns.ealing.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 students' 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

Learning platform

- Uploading of information on the schools' Learning Platform / restricted area of the web site 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/restricted area of the web site will only be accessible by members of the school community;
- In school, students are only able to upload and publish within school approved and closed systems, such as the Learning Platform/restricted area of the web site.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students.

School staff will ensure that in private use:

- No reference should be made in social media to students, parents / carers, other professionals 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 St Ann's School or the Local Authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school

- Only uses the LGfL supported services for video conferencing activity;
- Only uses approved or checked webcam sites;
-

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. In the near future we will be able to record site surveillance images. 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 may also use this footage to share with parents/carers and other professionals (with parental permission) to demonstrate barriers to learning and progress in order to promote student achievement.

5. 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.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - staff,
  - governors,
  - parents/carers

  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 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, network access and Learning Platform/restricted website area access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken 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 log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We don't use flash drives unless specific permission has been given and the drive has been checked. Members of staff would not be required to take any sensitive information off site.
- 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 google chrome education with its high security for remote access into our systems.
- We use secure dfe approved systems to transfer other data to schools in London, such as references, reports of children.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in secure locations and managed by DBS-checked staff.
- We store 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 / admin server(s).
- Paper based sensitive information is shredded, using a high specification shredder
- We are using secure file deletion software.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Staff should store their mobile phones in locked lockers during their working hours. Personal mobile phones should only be carried on the person by a staff member in exceptional circumstances and when permission has been specifically granted by a member of the SLT eg in family emergency situations.
- On no account should any mobile phone or personally owned device be taken into a vulnerable area on the school site eg toilets, changing areas.
- Mobile phones brought into school are entirely at the staff member, student's and 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 (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may turn on and use their phones during designated school breaks and not in view of students.
  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 not permitted during the working day.
- 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.
- 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.
- 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 but not in front of students. In an emergency situation when a staff member is expecting a personal call they may seek specific permission from a member of the SLT to use their phone at other than their break times.
- Staff and students' mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off at all times and locked away.
- School owned 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 the curriculum manager (Deputy Headteacher)

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 young person to have a mobile phone eg to reduce anxiety, promote independence.
- If a student needs to contact his or her parents or carers, they will be supported to use a school phone. Parents are advised not to contact their young person via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- 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.
- Staff are not permitted to use their own mobile phones or devices for contacting young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school mobile phone or access to the school telephone system where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off. Bluetooth communication should be switched off. Mobile phones or personally-owned devices will not be used during teaching periods unless permission has specifically been granted (for a time limited period) by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use school owned mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the curriculum manager.
- 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 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
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their young person as part of the school agreement form when their daughter / son joins the school
- We do not identify students 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 students;
- If specific student 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 (and where appropriate student permission) for its long term use
- The school blocks access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Where appropriate students 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.
- Where appropriate students 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 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.

USB, External Hard Drive and Personal devices

- Any personal device is not allowed to be used for school unless explicitly written agreement with model noted is given by the Headteacher.
- The School reserves the right to search the content of any personal 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.

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.

Reviewed 25.09.15

Date of next review September 2017