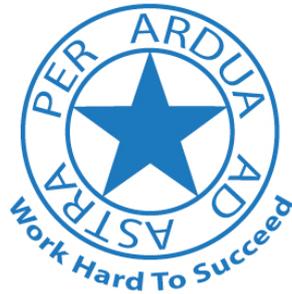


Garden Suburb Schools



Online Safety Policy

May 2017

Next Review - May 2018

This policy is part of our **Statutory Safeguarding Policy**. Any issues and concerns with online safety **must** follow our safeguarding and child protection processes.

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images

Appendices

- A1: Acceptable Use Agreement (Staff, Volunteers and Governors)

A2: Acceptable Use Agreement (Pupils - adapted for phase)

A3: Acceptable Use Agreement including photo/video permission (Parents)

A4: Protocol for responding to online 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

A5: Prevent: Radicalisation and Extremism

A6: Data security: Use of IT systems and Data transfer

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 Garden Suburb Schools with respect to the use of IT-based technologies
- Safeguard and protect the children and staff
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community
- Have clear structures to deal with online abuse such as online bullying (noting that these need to be 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content
 - Unlawful & Inappropriate use of content

Contact:

- Inappropriate disclosure of information and pictures on social media
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords
- Inappropriate contact either directly or via social media

Conduct:

- Aggressive behaviours including bullying
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (Recognising what constitute health & wellbeing risks associated with online use)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)
- Use of language appropriately

Scope

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

Roles and responsibilities

Head teacher

- Is adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance
- Leads a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding
- Takes overall responsibility for online safety provision
- Takes the role of Senior Information Risk Officer (SIRO) ensuring school's provision follows best practice in information handling (See Data Protection Policy)
- Ensures the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services
- Is responsible for ensuring that all staff receive suitable training in safeguarding and online safety
- Is aware of the appropriate safeguarding procedures to be followed in the event of an online safety incident
- Ensures suitable 'risk assessments' are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Receives regular monitoring reports from the Online Safety Co-ordinator/s
- Ensures that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager
- Ensures that Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

- Ensures that parents/carers are regularly informed
- Ensures that the school website includes relevant information.

Online Safety Co-ordinators and Designated Child Protection Lead

- Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents
- Promote an awareness and commitment to online safety throughout the school community
- Ensure that online safety education is embedded within the curriculum
- Liaise with school technical staff where appropriate
- Communicate with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Ensure that online safety incidents are logged as a safeguarding incident
- Facilitate training and advice for all staff
- Oversee any pupil surveys/pupil feedback on online safety issues
- Liaise with the Local Authority and relevant agencies
- Ensure they are regularly updated on online safety issues and legislation, and are aware of the potential for serious child protection concerns.

Governors/Safeguarding governor (including online safety)

- To ensure that the school has in place policies and practices to keep the children and staff safe online
- To approve and review the Online Safety Policy annually and/or whenever there are any new guidelines
- To review the policy's effectiveness every year
- To ensure that back up procedures and the Recovery plan are in place & effective
- To support the school in encouraging parents and the wider community to become engaged in online safety activities.

Computing Curriculum Leaders

- Oversee the delivery of the online safety element of the Computing curriculum.

Network Manager/Technician

- Report online safety related issues that come to their attention, to the Online Safety Coordinator
- Manage the school's computer systems, ensuring:
 - Systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)

- 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
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Ensure appropriate backup procedures and disaster recovery plans are in place
- Keep up-to-date documentation of the school's online security and technical procedures

Data and Information (Asset Owners) Managers (IAOs)

- To ensure that the data they manage is accurate and up-to-date
- Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
- The school must be registered with Information Commissioner

LGfL Nominated contact(s)

- To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant (See Data Protection Policy)

Teachers

- Embed online safety in the curriculum
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All staff, volunteers and contractors

- Read, understand, sign and adhere to the school staff Acceptable Use Agreement (AUA), and understand any updates annually. The AUA is signed by new staff on induction.
- Report any suspected misuse or problem to the online safety coordinator
- Maintain an awareness of current online safety issues and guidance e.g. through CPD
- Model safe, responsible and professional behaviours in their own use of technology
- At the end of the period of employment/volunteering staff return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Pupils

- Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- Understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
- Contribute to any 'pupil voice' / surveys that gathers information of their online experiences

Parents/carers

- It is the responsibility of Parents/carers to read, understand and promote the school's Pupil Acceptable Use Agreement with their child/children
- Should consult with the school if they have any concerns about their children's use of technology
- Should 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
- Parents/carers will be introduced to the policy as part of an Online Safety talk annually

Communication:

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

- Policy to be posted on the school website, staffroom and in classrooms
- Policy to be part of school induction pack for new staff
- The Online Safety policy will be disseminated to all staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety
- Staff and pupils are given information about infringements in use and possible sanctions
- Online Safety Coordinator acts as first point of contact for any incident

- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Head Teacher, unless the concern is about the Head Teacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting/nude selfie incident:

There should always be an initial review meeting, led by the designated safeguarding lead.

This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people

When assessing the risks the following should be considered:

- Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
 - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
 - Are there any adults involved in the sharing of imagery?
 - What is the impact on the pupils involved?
 - Do the pupils involved have additional vulnerabilities?
 - Does the young person understand consent?
 - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
 - If it is necessary to view the imagery in order to safeguard the young person - in most cases, imagery should not be viewed
 - What further information is required to decide on the best response
 - Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown
 - Whether immediate action should be taken to delete or remove images from devices or online services. If so, the legality for doing so will be checked with the LA.
 - Any relevant facts about the young people involved which would influence risk assessment
 - If there is a need to contact another school, college, setting or individual
 - Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

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

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

5. You have reason to believe a pupil(s) is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

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

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

Reviewing and Monitoring Online Safety

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school or outside the school's environment
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

Garden Suburb Schools:

- Have a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- Plan online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- Ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensure that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/ intellectual property rights;
- Ensure pupils only use school-approved systems and publish within appropriately secure/age-appropriate environments.

Staff and governor training

At Garden Suburb Schools, it is the responsibility of the Governing Body and the Head Teacher to

- Ensure that regular and up to date training is provided to all staff, volunteers and governors
- Make regular training available to staff on online safety issues and the school's online safety education program including a "refresher training session" at the beginning of each academic year
- Provide, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.
- Ensure that governors attend relevant LA training and/or are invited to in school staff training.

Parent awareness and training

At Garden Suburb Schools, It is the responsibility of the Head teacher to:

- Provide induction for parents which includes online safety;
- Run a rolling programme of online safety advice, guidance and training for parents including an Online Safety talk at the beginning of each academic year.

3. Expected Conduct and Incident management

Expected conduct

In Garden Suburb Schools, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- Understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- Know and understand school policies on the use of mobile and hand held devices including cameras.

Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- Should know and understand what the school's Online Safety Acceptable Use agreement
- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online Safety Acceptable Use agreement form

Incident Management

In Garden Suburb Schools:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- All members of the school 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;

- Monitoring, reporting and logging of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities - Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

Garden Suburb Schools:

- Inform all users that Internet/email use is monitored;
- Have the educational filtered secure broadband connectivity through the LGfL;
- Use the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Use USO user-level filtering where relevant;
- Ensure network health through use of anti-virus software (from LGfL);
- Use DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Use encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Work in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

Garden Suburb Schools:

- Use class log-ins for all users;
- Use guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Have additional local network monitoring/auditing software installed;
- 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;
- Have daily back-up of school data (admin and curriculum);
- Use secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#);
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the [EU data protection directive](#) where storage is hosted within the EU.

To ensure the network is used safely, our schools:

- Ensure staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network
- Make clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Have set-up the network with shared work areas for pupils, staff and office users;

- Show staff and pupils how to save work and access work from these areas;
- Require all users to log off/lock when they have finished working or are leaving the computer unattended;
- Ensure all equipment owned by the school and/or connected to the network has up to date virus protection;
- Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Make 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.
- Maintain equipment to ensure Health and Safety is followed;
- Ensure that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems;
- Do not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Have a clear disaster recovery system in place that includes a secure, remote off site back up of data. This will form part of the Recovery Plan;
- Use secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- 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);
- Ensure the wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- Ensure all IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- It is made clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised must change their password at the first opportunity and the school should be notified immediately
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

E-mail

Garden Suburb Schools:

- Provide staff with an email account for their professional use and makes clear that work email should only be used through work account and that personal e-mail should be through a separate account;

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that e-mail accounts are maintained and up to date
- Use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product plus direct email filtering for viruses.

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff will use the LGfL e-mail systems for professional purposes
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Head Teacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school website complies with statutory DFE requirements;
- 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;
- Photographs published on the website 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;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate
- 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, but to use the schools' preferred system for such communications
- Social networking sites are blocked using the school filtering system.
- Staff should not become "online friends" with parents/carers. In cases where a member of staff was an "online friend" with a parent/carers prior to their employment, any such friendship should be notified to the Head Teacher.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to schools matters or members of the school community;
- Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work
- Students are required to sign and follow our age appropriate pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission
- 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 Garden Suburb Schools:

- The Head Teacher is the Senior Information Risk Officer (SIRO)
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners
- 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 a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 3 minutes idle time
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content
- All servers are in lockable locations and managed by DBS-checked staff
- 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
- 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
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data
- We are using secure file deletion software.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices
- Visitors are not allowed to use their phones/mobile devices while on schools premises unless permitted by the Head Teacher, a member of the SMT or the business manager/Welfare officer
- No students should bring his or her mobile phone or personally-owned device into school unless they are "lone travellers" and parents/carers have informed the school by filling in the appropriate request form
- Student personal mobile devices, which are brought into school, must be turned off and handed into the school office on arrival at school. They must remain turned off and out of sight until the end of the day
- Any device brought into school and not handed over to the schools office at the start of the school day will be confiscated
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Staff members may use their phones in Staff Rooms during school break times
- The School reserves the right to search the content of any mobile devices *on* the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring. This will be done according to legal advice provided by the LA.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents/carers should not contact their child via their mobile phone during the school day, but contact the school office.
- Schools Trips & School Journey

Parents are advised that they should contact the school office, should any emergency occur.

Year 6 parents/carers will be informed by the school on the appropriate ways in which they can contact their children in case of emergency.

Digital images and video

In Garden Suburb Schools:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials
- 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, high profile use
- Annual schools/pupils photos: The schools will ensure that the contractor has the appropriate safeguarding requirements, especially regarding online use, in place before hiring.
- The schools blocks/filter access to social networking sites;
- Pupils are taught about how images can be manipulated in their online 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 computing 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. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Headteacher Infant School: _____ **Date:** _____

Headteacher Junior School: _____ **Date:** _____

Chair of Governors: _____ **Date:** _____

Date of Next Review: **May 2018**