Primary Advantage

Online safety and acceptable use policy

PRIMARY ADVANTAGE

SCHOOLS ACHIEVING MORE TOGETHER

Table of Contents

Table of Contents

1. Introduction and Overview

Rationale:
The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of IT-based technologies;
- Safeguard and protect the children and staff of our school;
- 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/or 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 which are cross referenced with other school policies;
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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

Content:

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

Contact:

- Grooming (sexual exploitation, radicalisation etc.);
- Online bullying in all forms;
- Social or commercial identity theft, including passwords

Conduct:

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information;
- Digital footprint and online reputation;
- Health and well-being (amount of time spent online (gambling, body image, 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 our school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy IT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils 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 online bullying, or other online 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. In the case of both acts, action can only be taken over issues covered by the published Pupil Discipline and Anti-Bullying Policy.

The school will deal with such incidents within this policy and the associated Pupil Discipline and Anti-Bullying policy and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision; • To take overall responsibility for data and data security (SIRO) ensuring school's provision follows best practice in information handling; • To ensure the school uses 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 online safety roles and to train other colleagues, as relevant; • To be aware of procedures to be followed in the event of a serious online safety incident; • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Co-ordinator / Officer; • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager). • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.

Online safety Co-ordinator / ICT co-ordinator Designated Child Protection Lead	• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents;
	• Promotes an awareness and commitment to e-safeguarding throughout the school community;
	• Ensures that online safety education is embedded across the curriculum
	• Liaises with school technical staff where appropriate;
	• To communicate regularly with SLT and the designated online safety Governor/committee 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 online safety incident;
	• To ensure that an online safety incident is logged as a safeguarding incident and is kept up to date;
	• Facilitates training and advice for all staff;
	• Oversee any pupil surveys / pupil feedback on online safety issues
	• Liaises with the Local Authority and relevant agencies;
	• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  ○ Sharing of personal data;
	  ○ Access to illegal / inappropriate materials;
	  ○ Inappropriate on-line contact with adults / strangers;
	  ○ Potential or actual incidents of grooming;
	  ○ Cyber-bullying and use of social media.

Governors	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online safety Policy and review the effectiveness of the policy. This will be carried out by the Governors /Local Advisory Boards receiving information about online safety incidents and monitoring reports; • To support the school in encouraging parents and the wider community to become engaged in online safety activities;

	• The role of the Governors (LDBS states an online safety governor) will include regular review with the Online safety Co-ordinator / Officer / IT Coordinator (including online safety incident logs, filtering / change control logs).
ICT Co-ordinator	• To oversee the delivery of the online safety element of the Computing curriculum; • To liaise with the online safety coordinator regularly.
Network Manager/ technician	• To report any online safety related issues that arise, to the online safety coordinator/IT co-ordinator; • To manage the school's computer systems, ensuring • - school password policy is strictly adhered to. 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; - 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 • 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 they 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; • That the use of the network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator /ICT Co-ordinator/ Officer /Headteacher for investigation / action / sanction; That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • 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.
Admin/Finance/ Data Manager	• 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 including maintaining the LGfL USO database of access accounts.
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities; • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extracurricular 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.
All staff and volunteers	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • To read, understand and help promote the school's online safety policies and guidance;

	• To read, understand, sign and adhere to this policy; • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices; • To report any suspected misuse or problem to the online safety coordinator; • To maintain an awareness of current online safety issues and guidance e.g. through CPD; • To model safe, responsible and professional behaviours in their own use of technology; • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. Exit strategy • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, 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 Appendices 3 & 4. (nb. at KS1 it would be expected that parents / carers would sign on behalf of the pupils); • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations; • To understand the importance of reporting abuse, misuse or access to inappropriate materials; • To know what action to take if they, or someone they know, feels worried or vulnerable when using online technology; • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices; • To know and understand school policy on the taking / use of images and on cyber-bullying; • To 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, 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; • To help the school in the creation/ review of online safety policies. • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
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; • 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 Agreement prior to using any equipment or the internet within school. • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

The responsibility for online safety is shared between the Headteacher, Safeguarding Nominated person and the ICT Co-ordinator at each school.

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

- Policy to be posted on the school website/staffroom/ classrooms;
- Policy to be part of school induction pack for new staff;
- Regular updates via email, staff meetings or bulletins and training on online safety for all 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 /Online safety Coordinator/Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework;
- Referral to LA / Police.
- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher;
- Complaints of online bullying are dealt with in accordance with our Pupil Discipline and Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.
- 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 Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:
UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:
There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

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

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

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

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

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

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

Review and Monitoring:
The Online safety & Acceptable Use Policy should be reviewed in conjunction with the following policies:

- Pupil Discipline and Anti-Bullying Policy;
- Safeguarding and Child Protection Policy;
- Social Media & Networking Policy;
- Asset Disposal Policy;
- FOI & Data Protection Policy;
- Records Management Policy;
- CCTV Policy;
- The school has an Online Safety Coordinator who will be responsible for document ownership, review and updates.
- The Online safety & Acceptable Use Policy will be reviewed every three years or when any significant changes occur with regard to the technologies in use within the school.
- The Online safety & Acceptable Use Policy has been written by the school IT Co-ordinator/Online safety Co-ordinator, has been reviewed by governors 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 Governors. All amendments to the school E-safeguarding Policy will be discussed in detail with all members of staff.

2. Education and Curriculum
Pupil online safety curriculum:
This school:

- Has 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, including:
  - To STOP and THINK before they CLICK;
  - To develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - To be aware that the author of a website / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - To know how to narrow down or refine a search;
  - (For older pupils) To understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - To understand why they must not post pictures or videos of others without their permission;
  - To know not to download any files – such as music files - without permission;
  - To have strategies for dealing with receipt of inappropriate materials;
  - (For older pupils) To understand why and how some people will 'groom' young people for sexual reasons;
  - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;

- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Will remind students about their responsibilities through Appendices 3 & 4;
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons;
- ensures 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;
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.

Staff and governor training:

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 online safety issues and the school's online safety education program through updates/ termly staff meetings etc.
- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training:

This school offers advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safety behaviour are made clear;
- Information leaflets; in school newsletters;
- Suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.
- provides induction for parents which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct:

In this school, all users:

- Are responsible for using the school IT and communication systems in accordance with this policy which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils);
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety & Acceptable Use 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.

Staff are responsible for reading the school's Online safety & Acceptable Use Policy and using the school IT and communication systems accordingly, including the use of mobile phones, and hand held devices.

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

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

Incident Management:

In this school:

- There is strict monitoring and application of the Online safety & Acceptable Use 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 online safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA;
- 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. Refer to Appendix 2.
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering:

This school:

- informs all users that Internet/email us is monitored;
- 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 adult content, race hate, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as DFE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;

- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment/ LGfL secure platforms such as J2Bloggy, etc
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids and Google Safe Search;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the IT Coordinator. Our system administrator logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

The DfE has published guidance for headteachers, school staff and governing bodies in terms of searching, screening and confiscation. Please visit DfE - Searching, screening and confiscation.

Network management (user access, backup):
This school:

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all confidential data within the school will conform to the UK data protection requirements;
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely;
This school:

- Ensures staff read and sign that they have understood the school's Online safety & Acceptable Use 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 / We also provide a different/use the same username and password for access to our school's network;
- All pupils have their own unique usernames and password which gives them access to the Internet and other services;

- 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;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day;
- Has set-up the network so that users cannot download executable files / programmes;
- Makes clear that staff are responsible for ensuring that all equipment owned by the school 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 / TA; equipment installed and checked by approved Suppliers / LA electrical engineers;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role (e.g. teachers access report writing module; SEN coordinator - SEN data);
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems (e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system);
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems (e.g. technical support or MIS Support), our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level/appropriate standards suitable for educational use;
- All computer equipment is installed professionally and regularly reviewed to ensure they meet 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.

Passwords policy:

- This school makes it clear that staff keep their password private, must not share it with others and must not leave it where others can find; If a password is compromised 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 private;
- We require staff to use strong passwords for access into our MIS system for information on data management please refer to the Records Management Policy.
- We require staff to change their passwords into the MIS, LGfL USO admin site, every 90 days/twice a year.
- We require staff using critical systems to use two factor authentication.

E-mail:

This school:

- Provides staff with an email account for their professional use using Google Mail, Microsoft Office 365 or LA, and makes clear personal email should be through a separate account;
- Provides highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils;
- Uses Londonmail with students as this has email content control;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@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 contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up to date;
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police;
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web;
- In accordance with the Data Protection Act 1998 the school reserves the right to right to monitor the use of these systems. Emails may be inspected at any time without notice where malpractice is suspected;
- 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.

Pupils:

- Pupils' e-mail accounts are intentionally 'anonymised' for their protection;
- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work;
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this;
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - That an e-mail is a form of publishing where the message should be clear, short and concise;
    - That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
    - To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - That they should think carefully before sending any attachments;
    - Embedding adverts is not allowed;
    - That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - Not to respond to malicious or threatening messages;
    - Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - That forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with. See Appendix 1.

Staff:

- Staff can only use the school e-mail systems on the school system;
- Staff only use school 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, named LA system. If there is no secure file transfer solution available for the situation, then the data/file must be protected with security encryption;
- 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 LA / school Agreement Form AUP to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website:

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

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

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.
- For the use of any school approved social networking will adhere to school's communications policy.
- The school's preferred system for social networking will be maintained in adherence with the Social Media Policy.

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 members of the school community;
- Personal opinions should not be attributed to the school 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.

Video Conferencing:

This school 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. The use of CCTV is clearly signposted in the school. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation;
- 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:

Please refer to the Records Management Policy and for more information in managing student data and Remote Back-Up Policy.

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We 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 areas 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 use encrypted flash drives if any member of staff has 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 RAv3 / 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 references, reports of children.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the London content.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We 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 Turn IT On's NAS Discover backup for disaster recovery on our servers.

- 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 out by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.
- 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

Personal mobile phones and mobile devices:

- **Mobile phones brought into school are entirely at the staff member, students & 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 personal mobile devices, which are brought into school, must be turned off (not placed on silent) and handed in at the office on arrival at school. They must remain in the office until the end of the day.**
- **All visitors are requested to keep their phones on silent and not use the phone around the school;**
- **The recording, taking and sharing of images, video and audio on any personal mobile phone is not permitted; except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.**
- **The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring;**
- **Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times;**
- **Mobile phones will not be used unless directed by the Headteacher for specific purposes (e.g. method of contact on a school trip);**
- **No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned;**

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices:

- Phones and devices must be handed to the school office at the beginning of each day;
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office;
- 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;
- Any device brought into school and used in breach of this policy will be confiscated.

- **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;
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose;
- If a member of staff breaches the school policy then disciplinary action may be taken;
- 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:**
  In this school:
  - We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
  - We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
  - If specific pupil photos (not group photos) are used on the school website, 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;
  - The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
  - Pupils are taught about how images can be manipulated in their 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, 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.

- **Recording of plays and events – Parents:**
  - Please see the appendices section for the school's guidance on recording of plays and events for parents.

- **Asset disposal:**
  - Please refer to the schools Asset Disposal Policy.

APPENDIX 1

Staff Acceptable Use Policy

This agreement covers the use of digital technologies in NAME OF SCHOOL Primary including email, internet, shared network drives, network resources, all software, electronic equipment and all systems.

- I will only use NAME OF SCHOOL Primary's digital technology resources and systems for professional purposes
- I will not reveal my password(s) to anyone
- I will follow 'best practice' advice in the creation and use of my password(s). If my password is compromised, I will ensure I change it
- I will not use anyone else's password, nor seek to discover it. If a colleague does reveal it to me, I will advise them to change it
- I will not allow unauthorised individuals to access any of NAME OF SCHOOL Primary's systems
- I will ensure all documents and digital resources are saved, accessed and deleted in accordance with the NAME OF SCHOOL Primary's network and data security and confidentiality protocols
- I will not engage in any online activity that compromises my professional responsibilities, code of conduct or professional boundaries
- My personal online communication tools, including mobile phones, will not be used with service users and I will not communicate or 'befriend' any service user using these methods, even if they have recently left or no longer use the service
- I will use only the approved email system for all email communication related to work at NAME OF SCHOOL Primary
- I will not browse, download or send material that could be considered offensive to colleagues or others
- I will report any accidental access to, or receipt of, inappropriate materials or filtering breach to the headteacher
- I will not download any software or resources that can compromise the network, that breach a user's copyright, or are not correctly licenced
- I will not publish or distribute work that is protected by copyright
- I will not connect a computer, laptop, notebook or other electronic device (including USB flash drive) to the network that does not have up-to-date anti-virus software
- I will not use personal digital cameras or camera phones for taking and transferring images of children/young people or staff/volunteers without written permission, and will use those images only for their intended purpose
- I will ensure that any personal social networking sites/blogs, Twitter, Instagram accounts, etc., that I create or actively contribute to are separate from my professional role
    - It is my responsibility to ensure that my use of social networking sites/blogs, etc., does not compromise my professional role, and will ensure my privacy settings are appropriate
- Any computer, laptop or electronic device loaned to me by Primary Advantage Federation or one of its schools is provided solely for professional use
- I will access NAME OF SCHOOL Primary's resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those resources
- Any confidential data that I transport from one location to another will be protected by encryption
- I will follow NAME OF SCHOOL Primary's data security protocols when using confidential data at any location
- Any information seen by me with regard to service users held within Primary Advantage Federation or one of its schools 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, e.g. Children's Social Care and/or the police

- It is my duty to support a whole organisation safeguarding approach and I will alert the NAME OF SCHOOL Primary's named child protection officer/relevant senior member of staff if the behaviour of any service user or member of staff/volunteer may be inappropriate or a cause for concern
- It is my responsibility to ensure that I remain up-to-date, read and understand the NAME OF SCHOOL Primary's most recent online safety policies
- I understand that all internet/network usage can be logged and this information can be made available to my line manager on request
- I understand that failure to comply with any aspect of this agreement could lead to disciplinary action

I agree to abide by this Acceptable Use Policy at all times

I wish to have a network account; an email account; and be connected to all systems that are relevant to my post at NAME OF SCHOOL Primary

Full name ..... (printed)

Job title .....

Signature ..... Date: .....

Authorised signature

I approve this user to be set-up on NAME OF SCHOOL Primary's computer systems

Full name ..... (printed)

Job title .....

Signature ..... Date: .....

APPENDIX 2 – Protocol for responding online safety incidents

Introduction

This guidance has been produce to support any member of staff who may have to deal with an online safety incident. An online safety incident may fall into one of the following types:

- **Inappropriate conduct**
  - Posting material on social networks which contravenes work guidelines
  - Inappropriate use of work email/internet
  - Inappropriate use of a mobile phone or electronic device
  - Password and account misuse (e.g. use of someone else's password or login)
- **Accessing unsuitable content**
  - Downloading and / or viewing illegal material
  - Downloading or view material unsuitable to the workplace
  - Deliberately accessing content that expresses extreme or racists views
- **Inadvisable contact**
  - Giving away too much information
  - Breaching client privacy
  - Unsettling or threatening messages; cyberbullying
  - Grooming behaviour or inappropriate contact with young people
  - Misrepresentation, defaming
- **Loss of confidential data**
  - As a result of theft or loss of computer, laptop or memory stick

First response to an online safety incident

Guidance for the first person at the scene of an online safety incident has been published in the form of a wallet card and poster. It presents the options succinctly under three headings:

- Step 1 - Preserve the evidence;
- Step 2 - Pass it on – seek help or support;
- Step 3 - Prevent it re-occurring.

Immediate action will involve making a judgement on the seriousness of the incident, preventing children coming into contact with unsuitable material and seeking appropriate help and support. Dealing with an incident may involve outside agencies or may be resolved by the school"s senior leadership and internal disciplinary procedures. Once the situation has been dealt with, then a full review will need to be initiated to take any action required to prevent the situation happening again.

Each of these areas is dealt with in more detail.

Step 1 – Preserving the evidence

If the incident involves the unacceptable, inappropriate or possibly illegal use of a computer, mobile phone or camera then it is important to preserve any evidence which may be currently on the device. Make sure that other children or young people do not come into contact with the device. In particular the discovery of indecent images or videos involving children should always result in taking advice from the police.

- **Immediate action to take:**
  - Turn off the monitor screen to prevent it being seen by bystanders or confiscate the device and prevent it being used again. Lock it away;
  - N.B. Schools have the power to confiscate and examine the contents of a mobile phone or device if they believe it has been used for any purpose which breaks school rules.
- **Preserving technical evidence:**
  - When preserving evidence it is advisable to seek technical support first and to have any actions either witnessed or supervised so that the chain of evidence can be corroborated. In addition make sure a record is kept of the step by step actions taken.
- **If the device is on:**
  - Take photos or video of the screen rather than printing it out (but print if you have to) unless the photograph would be of an indecent image of a child under 18, when taking a photograph would itself count as a criminal offence;
  - Save open files, emails or messages to external media. Avoid saving things locally (to local disk or internal memory);
  - Do not shut down the computer (which can remove evidence such as history information, temporary files etc);
  - Seek technical advice.
- **If the device is off:**
  - Make an external examination and take photos Do not start the computer/device;
  - Lock it away;
  - Seek technical advice;
  - If the content is on a shared network then the device should be taken out of service until an investigation can be completed by a technically competent person;
  - N.B. Someone acting in a technical capacity, with written instruction and supervision in a case that may become a criminal investigation has a defence in law when necessarily handling these materials to preserve evidence.

Step 2 – Pass it on

Seek help or support to decide if the incident needs to be referred to other agencies (DSP,LADO, HT, Police, parents, HR).

- **First contact with an incident could be:**
  - Something witnessed on a computer, mobile phone or camera;
  - A statement made by the victim;
  - Information from a bystander or witness about events or pointing to evidence that something untoward has happened;
  - Hearsay (rumour) about a potential situation;
  - Noticing an anomaly in a log, history e.g. using Internet Explorer.

- **Depending on the incident and the setting in which it occurred, report to:**
  - Line manager or a senior member of staff;
  - Safeguarding Officer;
  - Police 101;
  - Technical support;
  - Parents /carers;
  - Other external support.
- **All the following incidents indicate the need to consult external support:**
  - If there is a concern for the safety or wellbeing of a child, because there are suspicions, signs or symptoms of child abuse or harm, the normal Safeguarding Children Board Procedures must be followed.
- **Concern with regard to the behaviour of someone who works with children:**
  This may be because that person has:
  - Behaved in a way which has harmed a child, or may have harmed a child Possibly committed a criminal offence against or related to a child (e.g. by being abusive or grooming a child for later abuse);
  - Behaved towards a child or children in a way which indicates that he/she is unsuitable to work with children;
  - Has viewed or taken pictures of children or young people which make you feel uncomfortable;
  - The Local Authority Designated Officer must be informed. (N.B. this should be used for anyone who works with children, not just local authority employees).

- **Concerns about criminal behaviour:**
  The following triggers should result in the police being contacted:
  - Actual harm caused by violence, abuse or harassment or evidence that has occurred or is being incited or planned, including menacing behaviour, incitement, grooming or accessing indecent images
  - Theft or damage to property, including property kept online, and denial of service or access
  - Serious fraud and identity theft, including serious breaches of copyright
  - Distribution or possession of obscene, or hateful materials
  - Self-harm or severe distress caused by repeated acts which in themselves may not appear significant e.g. cyberbullying.
- There is specific Home Office guidance on the action police should take if a crime has been reported as having occurred in school. This indicates that all but serious or exceptional cases should be dealt with by school discipline procedures rather than being recorded as a crime.
- **A civil offence (which may also constitute an illegal act):**
  These are generally managed by the school disciplinary procedures or settled in the courts without police intervention and would require the support of HR. Triggers might include:
  - Data protection or privacy breaches (e.g. resulting from loss of a laptop or memory stick);
  - Professional or personal misconduct or negligence Libel, slander, defamation and misrepresentation;
  - Viewing inappropriate content;
  - Breaching acceptable use policies;
- **Other types of incidents:**
  - Other cases may breach the internal disciplines of acceptable use, behaviour or contract without falling into the categories of abuse, criminal or civil offence, and so can be dealt with by local procedures.
- **Collecting evidence and recording the incident:**
  - Contact details of any other witnesses should be noted and a written record made of what has been said and seen. Ensure that conversations are timed and dated.
- **Technicians:**
  - A technician may be asked to help respond to an incident by their employer (using the power the employer has to investigate employees under the Regulatory and Investigatory Powers Act) or by the head teacher (using powers given to them under education law) or by the police.
- **Acting under consented rights or with a written instruction a technician may be asked to:**
  - Collect evidence – hard disk, screen prints, a mobile phone logs, records or other instrumentation, statements;
  - Examine what has been collected to find evidence – e.g. look for files on a hard disk, numbers from a phone etc;
  - Treat or help recover from any harm caused – e.g. remove viruses, recover a system from a backup;
  - Give a statement as evidence – e.g. describing any work carried out on the hard disk, recovery of files from a backup and /or provision of encryption keys, calls to the ISP or emails to SNS provider, witness to a conversation or action taken;
  - Apply sanctions, such as removing internet privileges or restricting access on the computer network.

Step 3 – Prevent re-occurrence of the event by considering what action could be taken

Review policy and procedure:

Does the organisation have the correct Acceptable Use Policies (AUP) in place?

- **In order to act lawfully it is vitally important that actions are:**
  - As agreed in a written Acceptable Use Policy produced by someone who has authority in law (Headteacher and governors) OR
  - Under explicit (ad hoc) instruction from someone with appropriate authority in law OR
  - Are someone with explicit responsibilities in their job description (and associated competence) given by a lawful authority.
- **Acceptable Use and/or Acceptable Behaviour Policy, Home-school Agreement or Contract agreed by parents, staff and children in the setting must therefore include clauses that cover:**
  - Searching and monitoring of technology used in the setting Confiscation of technology whilst on the premises;
  - Privacy expectations, interception of communication and use of personal data in the setting;
  - Limits on what, where and when technology can be used and what for;
  - How infringements will be handled, including expected sanctions.
- **Providing support for the victim:**
  - Where an incident has involved the victimisation, harassment, alarm or distress of another pupil or member of staff support for the victim should be provided;
  - Where the incident involves a member of staff, appropriate support should be obtained. This might be the designated staff welfare member or the victim's union;
  - Where the victim is a pupil, contact family and carer and agree a suitable way forward to facilitate an effective closure for the victim to the incident.
- **In both instances:**
  - Implement the institution's 'restorative practices' procedures. Where the perpetrator agrees, participation in this process will be included as part of their reintegration programme following the incident;
  - Where "restorative practice" does not take place then other avenues to support the victim should be tried;
  - Ensure that the perpetrator is educated about the impact of their actions on the victim;
  - Ensure a fully documented case history of the incident is recorded;
  - Where material has been posted online about a victim, provide support in getting the material removed either through discussion with the poster of the material or contact with the service provider.

APPENDIX 3

Key Stage 1: Acceptable Use Agreement

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say	
6. I don't keep ~~**SECRETS**~~ just because someone asks me to	
7. I don't change **CLOTHES** in front of a camera	
8. I am **RESPONSIBLE** so never share private information	
9. I am **KIND** and polite to everyone	
10. I **TELL** a trusted adult if I'm worried, scared or just not sure	

My trusted adults are _____ at school

_____ at home and _____

My name is _____

APPENDIX 4

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, gams and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Signed: _____ Date: _____

APPENDIX 5
Parents Acceptable Use Agreement

<<School name>> regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding and Child Protection Policies, <<which can be found at…>>. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.

Your child/young person will be asked to read and sign an Acceptable Use Policy tailored to his/her age. Please read this carefully – it is <<attached to this form for reference // available online at XXXXX>>.

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

- the internet at school
- the school's chosen email system
- <<name any online 'managed learning environment', Google Classroom, Microsoft for Education tools, or similar>>
- IT facilities and equipment at the school

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

I understand that all internet and device use in school is subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used in the same manner as when in school.

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

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

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

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this. The impact of social media use is often felt in schools, and this is why we expect certain behaviours from pupils when using social media at all times.

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

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

I understand that my son/daughter has agreed in the pupil acceptable-use policy not to search for or share any material that could be considered offensive, harmful or illegal. This might include bullying or extremist/hate/discriminatory content.

I will support the school by promoting safe and responsible use of the internet, online services and digital technology at home. I will inform the school if I have any concerns.

Name(s) of pupil/student: _____

Parent / guardian signature: _____

Date: ___/___/___

APPENDIX 6 – Use of photographs and videos

DATA PROTECTION ACT 1998

PHOTOGRAPHS, VIDEOS AND WEBSITE

Photographs and videos are taken by the school for a variety of reasons, for example Sports Day, celebrations of achievement, fund raising events, educational visits, etc. We wish to keep a record of and publicise the many activities in which our pupils participate and therefore would like to display photographs throughout the school, including on the school's website. In some cases the Hackney Learning Trust or the local press may seek permission to use these photographs (they may also wish to take their own photographs of the pupils themselves).

Please tick

I consent to my child being photographed / videoed for the school's purposes including the school website? Yes ☐ No ☐

I consent to my child being photographed / videoed for Hackney Learning Trust, press/publicity and educational companies that might visit the school? E.g Local Library, Theatre & Events purposes. Yes ☐ No ☐

INTERNET

RESPONSIBLE USE AGREEMENT

The school uses Internet resources as part of the curriculum. It is School Policy not to allow unsupervised access to the Internet.

Please tick

I consent to my child having Internet access during **supervised** teaching sessions (including lunchtime and after school clubs)? Yes ☐ No ☐

Parent/Carer Name: ……..... Parent/Carer Signature: ……

Child's Name: …… Child's Year: ……

Date……

IF WE DO NOT RECEIVE A RESPONSE TO THIS LETTER WE WILL ASSUME YOU ARE HAPPY FOR YOUR CHILD TO HAVE THEIR PHOTOGRAPH TAKEN AND FOR US TO USE IT FOR SCHOOL AND HACKNEY LEARNING TRUST PURPOSES.

APPENDIX 7

Online safety incident reporting form

Details of person reporting the incident Name: Phone number: Email address:
Date of incident:
Where did the incident take place?
Description of the incident
Name(s) of those involved in the incident:
Age(s) of child(ren) involved:
Was the incident Child on child ☐ Child on adult ☐ Adult on child ☐ Adult on adult ☐ Staff member on child ☐
Type of incident Sexual ☐ Profanity ☐ Violence ☐ Bullying ☐ Grooming ☐ Other ☐ Please give details
How was the content accessed? School internet via a PC/laptop ☐ via a tablet ☐ via a mobile phone ☐ via email ☐ Tablet using alternative provider ☐ mobile phone using an alternative provider ☐ Via an internet browser ☐ via a social media website ☐ via an app ☐
What action was taken in relation to those involved in the incident?
What action was taken regarding the site/content accessed?
What follow-up action was taken? Referral to LADO ☐ Referral to Children's Social Care ☐ Advice to parents ☐ Police investigation ☐ Other ☐ Please provide details:

Policy written	January 2018
Adopted by Governing Body	September 2019
Review date	January 2021

The Governors have reviewed this policy with careful consideration of our approach to equalities as outlined in the Federation Equalities Policy.

We would like to acknowledge the work of other colleagues in drafting this policy. We have drawn on a range of sources including policies from other schools, good practice guides, published schemes and LA and Statutory guidelines where appropriate.

PRIMARY ADVANTAGE
SCHOOLS ACHIEVING MORE TOGETHER