E-Safety &
Data Security

<u>Including:</u> Electronic Information & Communication, Information Security, Cyber Security, Social Media, Use of Own Devices, Use of Cookies & CCTV

Policy Creation & Review	
Author(s)	Leon Dixon, Sue Ferguson, Judicium Education
Last review date	October 2023 *(updated school DPO & additional cyber security updates)*
Ratified by Governing Body	October 2021
Previous Review Date(s)	September 2021 September 2019 September 2018 *(GDPR compliance)* November 2016 June 2012
Next Review Date	October 2025

Please note that this policy pertains to practice in Ellen Wilkinson Primary and Little Ellies Childcare. Therefore the term 'school' is used to cover both of these provisions.

Contents

9. Equipment and Digital Content

- ❑ Personal mobile phones and devices
- ❑ Work devices
- ❑ Staff using own devices
- ❑ Digital images and video
- ❑ Asset disposal

Ellen Wilkinson Primary School
E-SAFETY & DATA SECURITY POLICY

1. Introduction and Overview

1.1 Aims

Our school aims to:

- ❏ Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- ❏ Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- ❏ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- ❏ Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

1.2 Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. 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. The Education Act 2011, has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The policy also takes into account the National Curriculum computing programmes of study.

1.3 GDPR – UK General Data Protection Regulation

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This documents sets out the measures taken by the school to achieve this, including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

This policy is written in accordance with the UK General Data Protection Regulation..

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the School who are required to familiarise themselves and comply with its contents. The School reserves the right to amend its content at any time.

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data. Therefore, it is regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the School'sGDPR Compliance Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the UK GDPR.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other mobile device tablets), Smart Phones, laptops, Chromebooks, mobile phones and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the GDPR.

Role	1.4 Key Responsibilities
Governing body & e-Safety Governor	The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, including the designated safeguarding lead (DSL). All governors will: ❑ Ensure that they have read and understand this policy ❑ Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2) ❑ To support the school in encouraging parents and the wider community to become engaged in e-safety activities The role of the E-Safety Governor will include: ❑ Regular review with the E-Safety Leads & Headteacher relating to e-safety issues.
Headteacher	The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. Duties include: ❑ To take overall responsibility for e-Safety provision ❑ To take overall responsibility for data and data security (SIRO) ❑ To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg LGfL ❑ To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant ❑ To be aware of procedures to be followed in the event of a serious e-Safety incident. ❑ To receive regular monitoring reports from the E-Safety Leads ❑ To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager) ❑ To ensure that an e-Safety incident log is kept up to date. ❑ To ensure compliance with all legislation requirements
Designated Safeguarding Lead	Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy. The DSL takes lead responsibility for online safety in school, in particular: ❑ Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school ❑ Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents ❑ Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy ❑ Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy ❑ Updating and delivering staff training on online safety ❑ Liaising with other agencies and/or external services if necessary ❑ Providing regular reports on online safety in school to the Headteacher and/or governing board This list is not intended to be exhaustive.
e-Safety Leads	❑ To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents ❑ To promote an awareness and commitment to e-safeguarding throughout the school community ❑ To ensure that e-safety education is embedded across the curriculum ❑ To liaise with school ICT technical staff ❑ To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues. ❑ To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident ❑ To facilitate training and advice for all staff

	❑ To liaise with the Local Authority and relevant agencies ❑ Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: ❑ sharing of personal data ❑ access to illegal / inappropriate materials ❑ inappropriate on-line contact with adults / strangers ❑ potential or actual incidents of grooming ❑ cyber-bullying and use of social media
Network Manager	❑ Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material ❑ To ensure the school's policy on web filtering is applied and updated on a regular basis ❑ To ensure LGfL/External Support is informed of issues relating to the filtering applied by the Grid ❑ To ensure that he/she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant ❑ that the use of the network, MLE and email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-Safety leads/Headteacher for investigation, action and where necessary, sanction ❑ Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly ❑ Conducting a full security check and monitoring the school's ICT systems on a weekly basis ❑ Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files ❑ To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date ❑ Ensuring that any online safety incidents are dealt with appropriately in line with this policy ❑ Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy ❑ To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. This list is not intended to be exhaustive.
Office Manager	❑ To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	❑ To embed e-safety issues in all aspects of the curriculum and other school activities ❑ To deliver the school's curriculum for e-safety. ❑ To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) ❑ To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	All staff, including contractors and agency staff, and volunteers are responsible for: ❑ Maintaining an understanding of this policy ❑ Implementing this policy consistently ❑ Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1) ❑ Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy ❑ Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

	❑ To report immediately any e-safety issues which arise within school, or are brought to the attention of the member of staff. ❑ To report any suspected misuse or problem to the e-Safety coordinator ❑ To model safe, responsible and professional behaviours in their own use of technology ❑ To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	❑ Read, understand, sign and adhere to the Pupil Acceptable Use Policy (NB. At KS1 it would be expected that parents/carers would sign on behalf of the pupils) ❑ To 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 and to understand how to do this. ❑ 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 handheld devices. ❑ To know and understand school policy on the taking/use of images and on cyber-bullying. ❑ To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school ❑ 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 e-safety policies
Parents/ Carers	❑ To support the school in promoting e-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 access the school website and related learning platforms in accordance with the relevant school Acceptable Use Agreement. ❑ To consult with the school if they have any concerns about their children's use of technology
External groups	❑ Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

1.5 Communication

❑ The policy will be communicated to staff, pupils, parents/carers and the wider school community in the following ways:

❑ Policy to be posted on the school website
❑ Policy to be part of school induction pack for new staff
❑ Acceptable use agreements discussed with pupils at the start of each year
❑ Acceptable use agreements to be issued to whole school community, usually on entry to the school
❑ Acceptable use agreements to be held in pupil and personnel files

1.6 Handling complaints:

❑ The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

❑ Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

❑ informing parents or carers;
❑ removal of Internet or computer access for a period;
❑ Referral to LA / Police.
❑ Our e-Safety lead acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

❑ Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school and LA child protection procedures.

1.7 Review and Monitoring

The e-safety policy is referenced from within other school policies and procedures including: Child Protection policy, Anti-Bullying policy, Behaviour policy, Complaints Policy, Staff Disciplinary Procedures, Data Protection Policies and Privacy notices.

The school has E-safety Leads who will be responsible for document ownership, review and updates.

❑ The e-safety policy will be reviewed when any significant changes occur with regard to the technologies in use within the school

❑ The e-safety policy has been written by the school e-safety lead, Network Manager and DSL.

❑ The DSL logs behaviour and safeguarding issues related to online safety.

❑ 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-safety policy will be discussed in detail with all members of the teaching staff.

2. Education and Curriculum

2.1 Pupil e-Safety curriculum

This school:

- Has a clear, progressive e-safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning focus for specific curriculum areas.
- Reminds students about their responsibilities through an end-user Acceptable Use Policy which every student will sign.
- Ensures staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming.
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

2.2 Staff and Governor training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- As part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safety policy and the school's Acceptable Use Policies.
- Staff will be shown how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.
- More information about safeguarding training is set out in our child protection and safeguarding policy.

2.3 Parent awareness and training

This school

❑ Runs a rolling programme of advice, guidance and training for parents, including:

○ Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear

○ demonstrations, practical sessions held at school giving suggestions for safe Internet use at home

○ Provision of information about national support sites for parents.

❑ Online safety will also be covered during parents' evenings.

❑ If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher.

3. Cyber-Bullying

3.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school positive behaviour policy.)

3.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The issue will also be addressed in assemblies.

Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. Helpful e-safety tips are also included in our weekly newsletters.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

3.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. Parents will always be notified in advance if this is being considered.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- ❏ Cause harm, and/or
- ❏ Disrupt teaching, and/or
- ❏ Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- ❏ Delete that material, or
- ❏ Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- ❏ Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

4. Expected Conduct and Incident management

4.1 Expected conduct

Information about expected conduct from all members of the school community can be found under the key responsibilities section of this policy, the AUP, staff code of conduct and related policies including the behaviour policy.

4.2 Incident Management

In this school:

- All members of our school community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g: the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school.
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- The police are contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4.3 How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the positive behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and severity of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

5. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

6. Managing the ICT infrastructure - Electronic Information & Communications Systems

6.1 Introduction

The School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the School who are required to familiarise themselves and comply with its contents. The School reserves the right to amend its content at any time.
This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data. Therefore, it is regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the UK GDPR.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other mobile device tablets), Smart Phones, laptops, Chromebooks, mobile phones and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

6.2 Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the type of user (staff or pupil);
- Ensures the network is healthy through use of Sophos anti-virus software (from LGfL) and the network is set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices where 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;
- 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;
- 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;
- 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 MLE or LGFL secure platforms such as J2Bloggy;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of LGFL as a key way to direct students to age / subject appropriate websites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg 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 pupils that they must report any failure of the filtering systems directly to the teacher. Staff should report them directly to the network manager. Our network manager 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.

6.2 Network management (user access, backup)

This school

- Uses individual log-ins for all users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Ensures the network manager is up-to-date with LGfL services and policies;
- Storage of all data within the school will conform to the UK data protection requirements

6.2.1 To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access;
- Provides staff access to the schools' management information system, controlled through a separate password for data security purposes and is limited to those users on the admin network;
- Provides pupils with an individual network login username;
- All pupils have their own unique username and password which gives them access to the MLE;
- Uses the London Grid for Learning Unified Sign-On (USO) system for MLE and LGFL access;
- 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;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by network manager/technician; equipment installed and checked by approved Suppliers / LA electrical engineers;
- Has separate curriculum and administration networks, with access to the Management Information System set-up so as to ensure staff users can only access modules related to their role;
- 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;
- Provides pupils and staff with access to content and resources through the approved Learning Platforms which staff and pupils access using their USO username and password;
- Makes clear responsibilities for the daily backup 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 backup 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 appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

6.3 Equipment Security and Passwords

- All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.
- Passwords are unique to each user and staff are required to select a password that cannot be easily broken and which contains at least 8 characters including both numbers and letters. All passwords should be considered complex
- Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the Network Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.
- If given access to the School e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Group and/or Network manager may do spot checks from time to time to ensure compliance with this requirement.
- Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.
- Logging off prevents another member of staff or a pupil accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.
- Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of Network Manager.
- On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The School reserves the right to require employees

to hand over all School data held in computer usable format.

- Members of staff who have been issued with a laptop, iPad (or other mobile device tablet) must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

6.4 Systems Use and Data Security

Members of staff should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the School's, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from Network manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screensavers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

All members of staff need to inform the Network Manager before sharing any data with any third parties so the School can carry out a Data Protection Impact Assessment (DPIA).

Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems. If in doubt, the employee should seek advice from a Network Manager or a member of the Senior Leadership Group.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming
- Instant messaging;
- Chat rooms;
- Social networking sites; and
- Personal - Web mail (such as Hotmail, Yahoo).

No device or equipment should be attached to our systems without the prior approval of the Network Manager or Senior Leadership Group. This includes, but is not limited to, any PDA or telephone, iPad (or other mobile device tablet), USB device, i-pod, digital camera, MP3 player or any other device. Devices with approval must be virus checked.

The School monitors all emails passing through its systems for viruses. Staff should be cautious when opening emails from unknown external sources or where for any reason an email appears suspicious (such as ending in '.exe' Network manager should be informed immediately if a suspected virus is received. The School reserves the right to block access to attachments to email for the purpose of effective use of the system and compliance with this policy. The School also reserves the right not to transmit any email message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the School's Systems and guidance under "E-mail etiquette and content" below.

6.5 E-mail etiquette and content

- E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.
- The School's e-mail facility is intended to promote effective communication within the business on matters relating to the School's business activities and access to the School's e-mail facility is provided for work purposes only.
- Staff are prohibited from using the School's email facility for personal emails at any time.
- Consideration should be taken about if email is the appropriate medium for a particular communication as the School encourages all members of its community to make direct contact with individuals rather than communicate by email wherever possible to maintain and enhance good working relationships.
- Messages sent on the e-mail system should be written as professionally as a letter message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the School's best practice.
- E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff

would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained on the appropriate file.

- All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the School. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the School in the same way as the contents of letters or faxes.
- E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. They may also be disclosed as part of dealing with subject access requests when they arise. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.
- Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The School standard disclaimer should always be used on every email.
- Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable
- Pupils will only have access to an internal school email account when it is linked to their curriculum work. Use of this facility will be monitored by the Network Manager.

6.6 Inappropriate communications

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages.If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should inform the Headteacher who will usually seek to resolve the matter informally. If an informal procedure is unsuccessful, you may pursue the matter formally under the School's formal grievance procedure. (Further information is contained in the School's Grievance Policy and Procedure.)

As general guidance, staff must not:

- Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private e-mails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the School;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals. [The message board public folder should be used for these purposes.]
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail, the internet or by other means of external communication which are known not to be secure;

The School recognises that it is not always possible to control incoming mail. The Network Manager should be made immediately aware of any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive so relevant action can be taken. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an email which has been wrongly delivered should return it to the sender of the message. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. The Headteacher should be informed as soon as reasonably practicable.

6.7 Use of the web and the internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not access any web page or any files from the School's system (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

- Staff should not under any circumstances use School systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.
- Staff should remember that text, music and other content on the internet are copyright works and should not download or e-mail such content to others unless certain that the owner of such works allows this.
- Staff should be aware that any personal use of the systems may also be monitored (see below) and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Inappropriate personal use of the School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

The School's website may be found at www.ellenwilkinson.newham.sch.uk. This website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership Group in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The School has published relevant information on its own shared network for the use of all staff. All such information is regarded as confidential to the School and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the School. Any exceptions to this must be authorised [jointly] by the author of the document(s) a member of the Senior Leadership Team.

6.8 Inappropriate use of equipment and systems

Access is granted to the web, telephones and to other electronic systems, for legitimate work purposes only.

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

A. Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
B. Transmitting a false and/or defamatory statement about any person or organisation;
C. Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
D. Transmitting confidential information about the School and any of its staff, students or associated third parties;
E. Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School;
F. Downloading or disseminating material in breach of copyright;
G. Copying, downloading, storing or running any software without the express prior authorisation of Network Manager
H. Engaging in online chat rooms, instant messaging, social networking sites and online gambling;
I. Forwarding electronic chain letters and other materials;
J. Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

6.9 School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school website complies with the statutory DfE guidelines for publications;
- 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 geo-data in respect of stored images

6.9.1 Cookies policy

What are cookies?

Cookies are small data files that are placed on your computer or mobile device when you visit a website. Cookies are widely used by online service providers to help build a profile of users. They are also used to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Some of this data will be aggregated or statistical, which means that we will not be able to identify you individually.

You can set your browser not to accept cookies and the websites below explain how to remove cookies from your browser. However, some of our website features may not function as a result.

Types of cookies

The cookies we place on your device fall into the following categories:

- **Session cookies**—these allow our website to link your actions during a particular browser session. These expire each time you close your browser and do not remain on your device afterwards
- **Persistent cookies**—these are stored on your device in between browser sessions. These allow your preferences or actions across our website to be remembered. These will remain on your device until they expire, or you delete them from your cache
- **Strictly necessary cookies**—these cookies are essential for you to be able to navigate our website and use its features. Without these cookies, the services you have asked for could not be provided
- **Performance cookies**—these cookies collect information about how you use our website, eg which pages you go to most often. These cookies do not collect personally identifiable information about you. All information collected by these cookies is aggregated and anonymous, and is only used to improve how our website works
- **Functionality cookies**—these cookies allow our website to remember the choices you make (such as your user name, language, last action and search preferences) and provide enhanced, more personal features. The information collected by these cookies is anonymous and cannot track your browsing activity on other websites

The cookies we use are:

How we use your cookies

EWPS may request cookies to be set on your computer or device. Cookies are used to let us know when you visit our website, how you interact with us and to make your experience using the school website better for you. The cookies we collect will differ depending on what you are looking at on our website. You are able to adapt your cookie preferences, but by blocking certain types of cookie it may mean that your experience on the website is impacted.

Consent to use cookies

We will ask for your permission (consent) to place cookies or other similar technologies on your device, except where these are essential for us to provide you with a service that you have requested (e.g. to enable you to put items in your shopping basket and use our check-out process).

There is a notice on our home page which describes how we use cookies and requests your consent to place cookies on your device.

How to turn off cookies

If you do not want to accept cookies, you can change your browser settings so that cookies are not accepted. If you do this, please be aware that you may lose some of the functionality of this website. For further information about cookies and how to disable them please go to the Information Commissioner's webpage on cookies: https://ico.org.uk/for-the-public/online/cookies/

6.10 Learning platforms

- Uploading of information onto any learning platform that the school is using must be authorised by the Network Manager.
- Photographs and videos uploaded to any learning platform will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems.

6.11 Social networking

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

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or carers;
- They do not engage in online discussion on personal matters relating to members of the school community ;
- Personal opinions should not be attributed to the school or local authority;
- Security settings on personal social media profiles must be set to maximum privacy to prevent access by unwanted parties.

Please see social media policy in the appendix for further details.

6.12 CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. For further details on how this is used please see the CCTV Statement (appendix 6).This can also be found in the Site and Personal Security Policy.

6.13 Clear desk expectations

Please see the staff general information handbook for the clear desk approach that staff are expected to follow.

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

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the School to achieve this, including to:-

- Protect against potential breaches of confidentiality;
- Ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- Support our GD{R Compliance Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- Increase awareness and understanding at the School of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they handle.

7.1 Introduction & General Principles

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. Staff are referred to the School's GDPR Compliance policy for further information.

All data stored on our IT Systems are to be classified appropriately (including, but not limited to personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the Office Manager & the Network Manager the appropriate security arrangements for the type of information they access in the course of their work.

All data stored within our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired and upgraded by the Network Manager or by such third party/parties as the Network Manager may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including but not limited to the security, integrity and confidentiality of that data) lies with the Network Manager in conjunction with the Office Manager

unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the Office Manager who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy). Please see the GDPR Compliance policy for further details.

7.2 Strategic and operational practices

At this school:

❑ The Head Teacher is the Senior Information Risk Officer (SIRO).
❑ We ensure staff know who to report any incidents where data protection may have been compromised.
❑ All staff are DBS checked and records are held in one central record.
❑ We ensure ALL the school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
❑ We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
❑ We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
❑ We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

7.3 Technical Solutions

❑ Staff have access to the multimedia drive to store photos and videos,
❑ We require staff to log-out of systems when leaving their computer unattended.
❑ We use encrypted USB 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.
❑ We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
❑ We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to LGFL content and our MLE.
❑ We store any Protect and Restricted written material in lockable storage cabinets in lockable storage areas.
❑ All servers are in lockable locations and managed by DBS-checked staff.
❑ We use LGFL remote backup for disaster recovery on our network (both admin, & curriculum servers)
❑ Due to this system (which operates daily) back-up tapes are no longer in use.
❑ All equipment is disposed of securely in accordance with the schools agreed procedures.
❑ Paper based sensitive information is shredded, using a cross cut shredder.

7.4 Physical Security and Procedures

Paper records and documents containing personal information, sensitive personal information and confidential information shall be positioned in a way to avoid them being viewed by people passing by as far as possible, e.g. through windows. At the end of the working day or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems is reviewed on a regular basis. If you find the security to be insufficient, you must inform the Premises Manager as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The following measures are taken by the School to ensure physical security of the building/s and storage systems:

- Regular checks of the buildings and storage systems to ensure they are maintained to a high standard.]
- An intercom system to minimise the risk of unauthorised people from entering the school premises.]
- The school gates close during certain hours to prevent unauthorised access to the building and an alarm system is set nightly.
- CCTV Cameras are in use at the School and monitored by the Premises Manager.

- Visitors are required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

7.5 Homeworking

Staff should not take confidential or other information home without prior permission of their line manager and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

- the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all confidential material that requires disposal is shredded or in the case of electrical material, securely destroyed as soon as any need for its retention has passed.

Please see the staff handbook for further guidance on UK GDPR & homeworking

8. Cyber Security

8.1 Introduction

- Cyber security has been identified as a risk for the School and every employee needs to contribute to ensure data security.
- The School has invested in technical cyber security measures, but we also need our employees to be vigilant and act to protect the School IT systems.
- The Network Manager] is responsible for cyber security within the School.
- If you are an employee, you may be liable to disciplinary action if you breach this policy.
- This policy supplements other data management and security policies, including our GDPR compliance policies and other sections of this document.

8.2 Purpose and scope

The purpose of this document is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as set out an action plan should the School fall victim to cyber-crime.This policy is relevant to all staff.

8.3 What is cyber-crime?

Cyber-crime is simply a crime that has some kind of computer or cyber aspect to it. It takes shape in a variety of different forms, e.g. hacking, phishing, malware, viruses or ransom attacks. The following are all potential consequences of cyber-crime which could affect individuals and/or individuals: -

- cost;
- confidentiality and data protection;
- potential for regulatory breach;
- reputational damage;
- business interruption; and
- structural and financial instability.

It is important, given the serious consequences above, to be careful not to be the victim of cyber-crime and to follow the guidance within this policy.

8.4 Cyber-crime prevention

This policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Network Manager can provide further details of other aspects of the school risk assessment process upon request.

The School has put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance to staff.

8.4.3 Technology solutions

The School has a variety of technical measures in place for protection against cyber-crime. They include:

- firewalls;
- anti-virus software;
- anti-spam software;
- auto or real-time updates on our systems and applications;
- URL filtering;
- secure data backup;
- encryption;

- deleting or disabling unused/unnecessary user accounts;
- deleting or disabling unused/unnecessary software;
- using strong passwords; and
- disabling auto-run features.

8.4.4. Controls and guidance for staff

All staff must follow the policies related to cyber-crime and cyber security as listed in the introduction to this policy and will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the School or any third parties with whom we share data.

All staff must:

- choose strong passwords
- keep passwords secret;
- never reuse a password;
- never allow any other person to access the school's systems using your login details;
- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the Network Manager has installed on their computer, phone or network or the School IT systems;
- report any security breach, suspicious activity, or mistake made that may cause a cyber security breach, to the Network Manager and Headteacher as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our data breach policy;
- only access work systems using computers or phones that the School owns. Staff may only connect personal devices to the visitor Wi-Fi provided;
- not install software onto your School computer or phone. All software requests should be made to the Network Manager and
- avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using School equipment or networks.

All staff must not misuse IT systems. The School considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against the School or using the School's systems;
- accessing inappropriate, adult or illegal content within School premises or using School equipment;
- excessive personal use of School's IT systems during working hours;
- removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy;
- using School equipment in a way prohibited by this policy;
- circumventing technical cyber security measures implemented by the School's IT team; and
- failing to report a mistake or cyber security breach.

8.5 Cyber-crime incident management plan

The incident management plan consists of four main stages:

1. Containment and recovery to include investigating the breach and utilising appropriate staff to mitigate damage and recover any data lost where possible.
2. Assessment of the ongoing risk to include confirming what data has been affected, what happened, whether relevant data was protected and how sensitive it is and identifying any other consequences of the breach/attack.
3. Notification to consider if the cyber-attack needs to be reported to regulators (for example the ICO) and/or colleagues/parents as appropriate.
4. Evaluation and response to consider any improvements to data security and evaluate future threats to security.

Where it is apparent that a cyber security incident involves a personal data breach, the school will invoke their Data Breach Policy rather than follow out the process in this section 5. Please see the Cyber Security Appendix to the Critical Incident Plan for more details

Equipment and Digital Content

9.1 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 handheld device brought into school.

❏ Staff may not use any mobile phone or mobile device except during their break times and in staff designated areas

unless with prior agreement of SLT.

❑ 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.

Any breach of the acceptable use agreement may trigger disciplinary action in line with the school's policies.

9.11 Students' use of personal devices

❑ The School strongly advises that student mobile phones should not be brought into school.

❑ Student mobile phones which are brought into school must be turned off (not placed on silent) and stored securely in an area designated by the class teacher on arrival at school. Mobile phones are only permitted to be brought to school by year 6 pupils who may come to and from school alone. This is so that they can maintain contact with their parents/carers during travel times.

❑ 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.

9.12 Staff use of personal devices

❑ Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

❑ Staff members may only use their phones during school break times. All staff and visitors must keep their phones on silent.

❑ Staff will be able to use the school phone where contact with parents or carers is required.

❑ Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. 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.

9.2 Staff using work devices outside school

Any member of staff wishing to use a work device outside of school must contact the network manager and sign the equipment log sheet. It is the member of staff's responsibility to sign the device back in upon its return including and accessories. Any faults must be reported. Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT Network Manager.

9.3 Staff using own devices

The School has implemented this policy to protect the School and all parties when using ICT and media devices. Staff are able to use devices at work and outside of work for work related activities provided the terms of this policy are met. The School reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

Mobile devices within the context of this policy includes any mobile phone, tablet, laptop, MP3/iPod or other device which is capable of connecting with the internet or mobile networks or taking image or sound recordings.

It is strongly recommended that wherever possible school provided devices are used and own device use should

be as an exception or due to necessary adaptation to support the individual.

This guidance is in addition to the School's Acceptable Use Policy.

All employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

9.3.1 Acceptable Use

- The School embraces the use of new and mobile technologies and acknowledges they are a valuable resource in the classroom having educational purposes.
- However, by accessing the School's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing so (including ensuring adequate security of that personal information).
- All staff who wish to use their own devices to access the School's network must abide by the AUP
- When in School staff should connect their device via the School's wireless network for security.
- When out of School, staff should access work systems on their mobile device using the approved school platforms through RM Unify.
- All internet access via the network is logged and, as set out in the Acceptable Use policy, employees are blocked from accessing certain websites whilst connected to the School network.
- The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by the Headteacher. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the School network.
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.

9.3.2 Non-Acceptable Use

Any apps or software that are downloaded onto the user's device whilst using the School's own network is done at the users risk and not with the approval of the School. Devices may not be used at any time to:

- Store or transmit illicit materials;
- Store or transmit proprietary information belonging to the school;
- Harass others;
- Act in any way against the School's acceptable use policy and other safeguarding and data related policies.
- Technical support is not provided by the School on the user's own devices

9.3.3 Devices and Support

Smartphones including iPhones and Android phones are allowed (the list should be as detailed as necessary including models, operating systems, versions). Again create a detailed list of approved smartphones and include them in an appendix attached at the end of this policy, e.g. Appendix D).

Tablets including iPad and Android are allowed (the list should be as detailed as necessary including models, operating systems, versions, etc. Again create a detailed list of tablets and include them in an appendix attached at the end of this policy, e.g. Appendix E).

Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

9.3.4 Security

In order to prevent unauthorised access, devices must be password/pin/fingerprint protected using the features of the device and a strong password is required to access the School network.

When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example through password protection and cloud back up) , keeping information confidential (for example by ensuring access to emails or sensitive information is password protected) and maintaining that information.

The School does not accept responsibility for any loss or damage to the user's device when used on the School's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).

Staff are prevented from installing email apps which allow direct access to School emails without use of a login/password.

If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device.

In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the School's data/cyber breach policy using the staff reporting portal.

The School may require access to a device when investigating policy breaches (for example to investigate cyber bullying).

Staff are not permitted to share access details to the School's network or Wi-Fi password with anyone else.

The School will not monitor the content of the user's own device but will monitor any traffic over the School system to prevent threats to the School's network.

9.3.5 Disclaimer

- The School reserves the right to disconnect devices or disable services without notification.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the School's policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The School reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

9.4 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;
- 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;
- Pupils are taught about how images can be manipulated in their e-Safety education programme;
- 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 that reveal 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.

9.5 Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed.
- 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.

Appendices

1. **Acceptable Use Agreement (Staff)**
2. **Acceptable Use Agreement (Parents+KS2 Pupils)**
3. **Acceptable Use Agreement (KS1 Pupils)**
4. **Permissions form (Parents)**
5. **Social Media Policy**
6. **CCTV Statement**

Appendix 1 - Acceptable Use Agreement (Staff)

Acceptable Use Agreement

Covers use of all digital technologies in schools i.e. email, internet, network resources, learning platforms, cloud services, software, communication tools, social networking, mobile devices, equipment and systems.

General

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the school.
- I will only use any LA / school / company system I have access to in accordance with their policies
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- I agree to follow the E-Safety & Data Security policy & GDPR Compliance policy.

Safeguarding

- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I will inform the Network Manager and/or Headteacher immediately if I am concerned about any online content that may be inappropriate.
- I understand that all Internet usage and network usage can be logged and this information could be made available to my manager on request.

Security

- I will not reveal my password(s) to anyone.
- I will ensure my password has adequate complexity (includes upper case, lower case, numbers and symbols) and change them regularly. If my password is compromised, I will ensure I change it promptly.
- I will not allow unauthorised individuals to access email/internet/intranet/network or other school systems
- I will ensure all documents; data etc are printed, saved, accessed and deleted. Dispose of securely in accordance with the school's network and data security protocols.
- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security systems or are not adequately licensed
- I will not connect any device (PC/Laptop/iPad) (including USB flash drive) to the network that does not have up to date anti-virus software
- I will only access school resources remotely using the approved system and follow e-security protocols to interact with them
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption, securely transported and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me in regards to staff or pupil information, held within the school's information management system, will be kept private and confidential EXCEPT when it is deemed necessary that I am required by law to disclose such information to the appropriate authority
- I will lock my device (PC/iPad) when not in use and not display any personal information on my IWB such as LGFL Emails.
- I will switch off my equipment when leaving it unattended for long periods of time.
- I understand that internet encrypted content (via https protocol) may be scanned for security and/or safeguarding purposes
- I understand that all internet and network traffic usage can be logged and this information can be made available to the Head/ DSL / Company on their request

Behaviours

- I will not engage in any online activity that may compromise my professional responsibilities or integrity
- I will not support or promote extremist organisations, messages or individuals
- I will not browse, download or send material that is considered offensive or of an extremist nature
- I will report any accidental access to, or receipt of, inappropriate materials, or filtering breach or equipment failure to the appropriate line manager/Headteacher.
- I will check copyright and not publish or distribute any work of pupils or staff including images, music and videos that is protected by copyright without seeking the author's prior permission.
- I will use the school's learning platform or cloud services in accordance with establishment protocols
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home.
- I will use the LT help form to log any IT issues that I need to raise

- I will ensure that any equipment used is returned to it's allocated storage

Google drive & school network

- I will use the shared google drive in accordance with the handbooks including where and what is stored on this facility
- I will report any anomalies or documents that have been inappropriately shared with other users (either accidentally or deliberately)
- I will not store personal information on shared drives
- ~~I will not save information on the school networks (google only)~~
- I will not use the school network as a main source for storing my data (google only)
- I will ensure I have access to the staff portal
- I will report any data breach and/or suspicious phishing emails on the relevant reporting forms.

Communication

- I will only use the approved email system(s) for any school business (LGFL Webmail)
- I will follow school email etiquette (see E-Safety & Data Security policy)
- I will inform the Network Manager and/or Headteacher if I receive any email which could be deemed offensive, inappropriate or potentially criminal.
- I will ensure I delete my work emails that are completed at least annually.

As general guidance, staff must not:

- Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private e-mails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the School;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Sell or advertise using the systems;
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure;

Social Media

- I will ensure that any private social networking sites / blogs / websites that I create or actively contribute to are not confused with my professional role and do not compromise myself, the school or the company
- I will abide by safeguarding rules regarding social media and not contact ex pupils/pupils from the school.
- Staff must not take photos or posts from social media that belong to the School for their own personal use.
- Staff should not use a work email address to sign up to any social media and any personal social media page should not make reference to their employment with the Trust (excluding LinkedIn, where prior permission is sought from the Headteacher.

Protecting our business reputation

- Staff must not post disparaging or defamatory statements about:
    - The School;
    - Current, past or prospective Staff
    - Current, past or prospective pupils
    - Parents, carers or families of (iii)
    - The School's suppliers and services providers; and
    - Other affiliates and stakeholders.

- Staff must not use the School's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Head Teacher.

GDPR

- I will ensure that I follow the GDPR policies and procedures in all respects in relation to my digital usage (further guidance is also available in the staff general information handbook)
- I will lock my computer screen when it is not in use

Equipment

- I understand that all electronic equipment must be signed out with the authorisation of the Network Manager.
- I understand that I may be charged for any repairs or replacement for equipment as a result of inappropriate and/or careless use (including accessories) - please see staff handbook for details.
- I will keep any 'loaned' equipment up-to-date, using the school's recommended system.
- I agree and accept that any device such as PC, laptop or iPad, loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any 'significant personal use' as defined by HM Revenue & Customs.
- I will follow the school's policy on use of mobile phones and devices in school

Acceptable Use Policy (AUP) Agreement Form

By electronically signing the agreement document you are agreeing;

- To abide by all the points above and any future amendments you are made aware of in advance.
- That you understand that you have a responsibility for your own and others online safeguarding and undertake to be a 'safe' and responsible digital technologies user.

Failure to comply with this agreement could lead to disciplinary action

Signature…….. Date……

Full Name …….. (Printed)

Job title/role……

Appendix 2 - Acceptable Use Agreement (KS2)

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

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.

3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I don't do live videos (live streams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I will help keep the school safe*** – I will not use USB drives unless permitted to do so by a teacher in school.

20. ***I respect the planet*** – I will not do any personal printing nor will I waste paper or print unnecessarily.
21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
22. ***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.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.
25. ***I am a caretaker*** – I will look after computing equipment at school and at home. I will not damage or change any settings on the computers or tablet devices.

Pupils constantly choosing not to follow these expectations will be warned and subsequently, may be denied further access to the IT facilities until a better understanding of the acceptable use at EWPS is demonstrated.

~~~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to the Network Manager or a trusted adult: at school that includes my class teacher _____

Outside school, my trusted adults are _____

Signed: _____ **Date:** _____

For parents/carers

- To find out more about online safety, you can read Ellen Wilkinson Primary School's full Online Safety Policy https://www.ellenwilkinson.newham.sch.uk/ParentZone/POLICIES/SAFEGUARDING for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).
- For E-Safety tips and help please visit https://www.ellenwilkinson.newham.sch.uk/ParentZone/E-SAFETY TIPS

Appendix 3 - Acceptable Use Agreement (KS1)

My name is _____

To stay SAFE online and on my devices, I follow the Digital 5 A Day and:
~~~~~~~~~~~~~~~~~~~~~~

1. I only **USE** devices or apps, sites or games if a trusted adult says so	●
2. I **ASK** for help if I'm stuck or not sure	●
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused	●
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	●
5. I look out for my **FRIENDS** and tell someone if they need help	●
6. I **KNOW** people online aren't always who they say they are	●
7. Anything I do online can be shared and might stay online **FOREVER**	●
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	●
9. I don't change **CLOTHES** in front of a camera	●
10. I always check before **SHARING** personal information	●
11. I am **KIND** and polite to everyone	●

My trusted adults are:

_____ **at school** _____ **at home**

For parents/carers

- To find out more about online safety, you can read Ellen Wilkinson Primary School's full Online Safety Policy https://www.ellenwilkinson.newham.sch.uk/ParentZone/POLICIES/SAFEGUARDING for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).
- For E-Safety tips and help please visit https://www.ellenwilkinson.newham.sch.uk/ParentZone/E-SAFETY TIPS

Appendix 4 - Parental Consent

Summary of permissions & agreements for my child

Name of child: _____

Date of birth: _____

UPN: _____

I agree the following permissions for my child:

Permissions – Visits and Events	Yes	No
All local visits (walking distance)		
All school visits (including those involving public transport) *(permission will always be asked separately for residential visits and /or visits abroad)*		
Participation and attendance at any competitive events *(e.g. sports competitions, art shows, writing competitions)*		
I do want the school to provide a packed lunch *(this will be free if they are entitled to free school meals or part of the mayors initiative, otherwise there will be a charge)*		
For staff to supervise my child applying sunscreen		

Permissions – Photos & Publicity	Yes	No
Use of my child's photograph, image and name within the school *(e.g. displays, class books, digital signage etc)*		
Use of my child's photograph, image and name for school publicity *(e.g. prospectus, displays)*		
Use of my child's photograph/image by other agencies *(e.g. news reports, local press, LA documentation)*		
Use of my child's photograph, image and name on the school website *(e.g Group shots, a piece of their work is being used or if they hold a positions of responsibility such a House captain)*		

Please note that children's individual image and their name would never be used together outside of the school environment for safeguarding reasons.

Permissions – Communication	Yes	No
Receive the newsletter and general school information by email		
Have your child's name used in the newsletter *(e.g. star of the week, participation in sporting competitions)*		
Receive general information texts from the school		
Receive first aid record by email		
Receive useful medical information from the NHS via the school		

I agree the following:

Agreement Area	Please tick
To follow the school's leave request procedure	
To abide by Internet Acceptable Use agreement	
To support the school's Anti Bullying Charter *(which will be reissued to me if any changes are made)*	

Agreement Area – Information Provided	Please tick
I agree I have received a copy of the following information ● **Information for parents** ● **Privacy Notice** ● **Attendance Information** ● **School Leave Request Information** ● **Safeguarding Information** ● **Collection Policy** ● **Anti-Bullying Charter** ● **Internet Acceptable Use Agreement**	

I understand and agree that the permissions I have given are valid for the entire time my child attends Ellen Wilkinson Primary School. I realise it is my responsibility to inform the school in writing of any changes I wish to make to these permissions. In return the school will notify me in writing of any changes to the documents. I have agreed to.

I also confirm that I have parental responsibility for this child.

Signed:_____ (adult with parental responsibility)

Name:_____ (please print)

Date: _____

Appendix 5 - Social Media Policy

Introduction

This policy applies to all School staff regardless of their employment status. It is to be read in conjunction with the School's Electronic Communications Policy. This policy does not form part of the terms and conditions of employee's employment with the School and is not intended to have contractual effect. However, it does set out the School's current practices and required standards of conduct and all staff are required to comply with its contents. Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the School's Disciplinary Policy and Procedure.

This policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

Purpose of this Policy

The School recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, X (formerly Twitter), LinkedIn, blogs, Instagram, TikTok, WhatsApp and Wikipedia. However, staff use of social media can pose risks to the School's confidential and proprietary information, its reputation and it can jeopardise our compliance with our legal obligations.

To minimise these risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate work related purposes, all school staff are required to comply with the provisions in this policy.

Who is covered by this policy?

This policy covers all individuals working at all levels and grades within the school, including senior managers, officers, governors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as Staff in this policy).

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

Scope and Purpose of this Policy

This policy deals with the use of all forms of social media including Facebook, LinkedIn, X (formerly Twitter), Wikipedia, Instagram, TikTok, WhatsApp and all other social networking sites, and all other internet postings, including blogs.

It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal.

Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether the School's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to cooperate with our investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Personnel responsible for implementing the policy

The Board of Governors have overall responsibility for the effective operation of this policy, but have delegated day-to-day responsibility for its operation to the Headteacher.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Headteacher in liaison with the Network Manager.

All senior school staff have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All school staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Headteacher in the first instance. Questions regarding the content or application of this policy should be directed by email to the Headteacher.

Compliance with related policies and agreements

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

a) Breach our Electronic information and communications systems policy;

b) Breach our obligations with respect to the rules of relevant regulatory bodies;

c) Breach any obligations they may have relating to confidentiality;

d) Breach our Disciplinary Rules;

e) Defame or disparage the School, its Staff, its pupils or parents, its affiliates, partners, suppliers, vendors or other stakeholders;

f) Harass or bully other Staff in any way or breach our Anti-harassment and bullying policy;

g) Unlawfully discriminate against other Staff or third parties or breach our Equal opportunities policy;

h) Breach our Data protection policy (for example, never disclose personal information about a colleague online);

i) Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

j) Breach our obligations for Keeping Children Safe in Education

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the school and create legal liability for both the author of the reference and the organisation.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Personal use of social media

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.

Staff should not use a work email address to sign up to any social media. Staff personal social media pages should not make reference to their employment with the school (excluding LinkedIn, where prior permission is sought from Headteacher]).

Staff must not take photos or posts from social media that belong to the School for their own personal use.

Monitoring

The contents of our IT resources and communications systems are the school's property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

The school reserves the right to monitor, intercept and review, without further notice, Staff members activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes. By your acknowledgement of this policy consent to such monitoring of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The school may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

All staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the School.

Educational or Extra Curricular Use of Social Media

If your duties require you to speak on behalf of the School in a social media environment, you must follow the protocol outlined below.

The Headteacher may require you to undergo training before you use social media on behalf of the School and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the School for publication anywhere, including in any social media outlet, you must direct the inquiry to the Headteacher and must not respond without advanced written approval.

Recruitment

The School may use internet searches to perform pre employment checks on candidates in the course of recruitment. Where the School does this, it will act in accordance with its data protection and equal opportunities obligations.

Responsible use of social media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

Photographs for use of Social Media

Any photos for social media posts may only be taken using school cameras/devices or devices that have been approved in advance by a member of the SLT. Where any device is used that does not belong to the School all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the School.

Staff Protocol for use of Social Media

Where any post is going to be made on the school's own social media the following steps must be taken:

1. Ensure that specific permission from the child's parent has been sought before information is used on social media. Note: A parent may have provided permission for one social media platform, but not another. Staff should ensure that the appropriate permission is specific.
2. Ensure that there is no identifying information relating to a child/children in the post - for example any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work. The School should seek additional consent to include any names when posting on social media
3. The post must be a positive and relevant post relating to the children, the good work of staff, the School or any achievements.
4. Social Media can also be used to issue updates or reminders to parents/guardians. The Headteacher will have overall responsibility for this. Should you wish for any reminders to be issued you should contact the main office to ensure that any post can be issued.
5. The proposed post must be presented to a member of the SLT for confirmation that the post can 'go live' before it is posted on any social media site.
6. The office staff will post the information, but all staff have responsibility to ensure that the Social Media Policy has been adhered to.
7. Personal information shared/published on social media will be required to be disclosed under a subject access request.

Protecting our business reputation

Staff must not post disparaging or defamatory statements about:

i. The School;

ii. Current, past or prospective Staff as defined in this policy

iii. Current, past or prospective pupils

iv. Parents, carers or families of (iii)

v. The School's suppliers and services providers; and

vi. Other affiliates and stakeholders.

vii. Current, past or prospective governors

Staff should also avoid social media communications that might be misconstrued in a way that could damage the School's reputation, even indirectly.

If Staff are using social media they should make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than School e-mail address when communicating via social media.

Staff are personally responsible for what they communicate in social media. Staff should be mindful that what they publish might be available to be read by the masses (including the School itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before they post content.

If Staff disclose directly or indirectly their affiliation to the School as a member of Staff whether past, current or prospective, they must also state that their views do not represent those of the School.

Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.

Staff must avoid posting comments about confidential or sensitive School related topics. Even if staff make it clear that their views on such topics do not represent those of the School, such comments could still damage the School's reputation and incur potential liability.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they have discussed it with his Line Manager or Head of Department.

If a member of staff sees content on social media that disparages or reflects poorly on the School, including its Staff, pupils, parents, service providers, stakeholders or governors, they are required to report this in the first instance to the Headteacher without unreasonable delay. All staff are responsible for protecting the School's reputation.

Respecting intellectual property and confidential information

Staff should not do anything to jeopardise School confidential information and intellectual property through the use of social media.

In addition, Staff should avoid misappropriating or infringing the intellectual property of other School's, organisations, companies and individuals, which can create liability for the School, as well as the individual author.

Staff must not use the School's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Headteacher.

To protect yourself and the School against liability for copyright infringement, the Staff member should, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Headteacher in the first instance before making the communication.

Respecting colleagues, pupils, parents, clients, service providers and stakeholders

Staff must not post anything that their colleagues, (past and/or current), pupils (prospective and/or current), parents, service provider, stakeholders or governors may find offensive, including discriminatory comments, insults or obscenity.

Staff must not post anything relating to colleagues, (past and/or current) or pupils, parents (prospective and/or current) service providers, stakeholders or governors without their advanced written permission.

Monitoring and review of this policy

The Headteacher shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice. The Board of Governors has responsibility for approving any amendments prior to implementation.

The Headteacher has responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

If staff have any questions about this policy or suggestions for additions that they would like to be considered on review, they may do so by emailing the Headteacher in the first instance.

Appendix 6 - CCTV Statement

Introduction

The school recognises that CCTV systems can be privacy intrusive.

Review of this statement shall be repeated regularly and whenever new equipment is introduced a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

Objectives

The purpose of the CCTV system is to assist the school in reaching these objectives:

(a) To protect pupils, staff and visitors against harm to their person and/or property.

(b) To increase a sense of personal safety and reduce the fear of crime.

(c) To protect the school buildings and assets.

(d) To support the police in preventing and detecting crime.

(e) To assist in identifying, apprehending and prosecuting offenders.

(f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence

(g) To assist in managing the school.

Purpose of this document

The purpose of this document is to regulate the management, operation and use of the CCTV system (closed circuit television) at the school. The CCTV system used by the school comprises of:

CAMERA TYPE	LOCATION	SOUND	RECORDING CAPACITY	SWIVEL / FIXED
1	School & House 5 x internal & 11 external	N	Y	F
2	West Building 1 internal & 11 external	N	Y	F

CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

CCTV Cameras are installed in such a way that they are not hidden from view. Signs are predominantly displayed where relevant, so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

Statement of Intent

- The CCTV system will seek to comply with the requirements of both the Data Protection Act and the most recent Commissioner's Code of Practice.
- The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.
- The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.
- Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
- Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.
- The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
- Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.
- Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.
- CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 30 days.
- Recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed)

and the incident to be investigated. In the absence of compelling a need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than [30 calendar days].

System Management

- Access to the CCTV system and data shall be password protected.
- The CCTV system will be administered and managed by Janice Connor (Facilities & Finance Manager) who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the system will be managed by [Simon Sutton – Premises Manager].
- Recordings only viewed after a given incident and by designated staff (Premises Manager, Finance & Facilities Manager, Network Manager & SLT) this has to be agreed by at least 1 SLT & 1 other authorised member of staff.
- The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.
- The CCTV system is designed to be in operation 24 hours each day, every day of the year, though the school cannot guarantee that it will be working at all times.
- The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.
- Cameras have been selected and positioned so as to best achieve the objectives set out in this statement in particular by proving clear, usable images.
- Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.
- Where a person other than those mentioned previously requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.
- Details of all visits and visitors will be recorded in a system log book including time/data of access and details of images viewed and the purpose for doing so.

Downloading Captured Data Onto Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -

(a) Each download media must be identified by a unique mark.

(b) Before use, each download media must be cleaned of any previous recording.

(c) The System Manager will register the date and time of download media insertion, including its reference.

(d) Download media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.

(e) If download media is archived the reference must be noted.

(f) If downloaded media is put onto a device, the device will be encrypted and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any download media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the download media (and any images contained thereon) remains the property of the school, and download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.

Applications received from outside bodies (e.g. solicitors or parents) to view or release images will be referred to the school's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's data protection officer.

Complaints About The Use Of CCTV

Any complaints in relation to the school's CCTV system should be addressed to the school DPO who is the Office Manager.

Request For Access By The Data Subject

The Data Protection Act provides Data Subjects – those whose image has been captured by the CCTV system and can be identified - with a right to data held about themselves, including those obtained by CCTV. Requests for such data should be made to the school DPO who is the Office Manager

Public Information

Copies of this statement will be available to the public from the school office.