Newham PRUs

Tunmarsh School, New Directions PRU, RIET

Head Teacher: Kirsten MacLeod

Newham PRUs

Online Safety Policy

For LGFL and RM CC4 Network

Policy created by **Roman Kutereba: April 2017**
Reviewed policy agreed by MC on: **June 2017**
Reviewed policy shared with staff on: **June 2017**
Policy to be reviewed again on: **September 2017**

Newham PRUs sites:

- Tunmarsh School (including Outreach provision)
- New Directions
- Coburn Unit
- RIET

To be reviewed in 2017 to take into account any review of the RM CC4 network (installed 09.2014) and with regard to the hardware and software refresh summer 2017. Also, to take into account any changes instigated by the DfE in relation to best practice in ICT and online safety. Review of any 'agreement' documents so that they are fit for purpose across all provisions that constitute Newham PRUs.

Contents

Appendices:

1. Document information
2. Acceptable Use Policy for ICT – Staff Agreement
3. Acceptable Use Policy for ICT – Pupil Agreement

References:

1. LGfL online-safety https://www.lgfl.net/online-safety/
2. Handling infringements http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf
3. Search & Confiscation guidance DfE https://www.gov.uk/government/publications/searching-screening-and-confiscation
4. Radicalisation: https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty
5. Cyberbullying: https://www.gov.uk/government/publications/preventing-and-tackling-bullying
6. Sexual exploitation https://www.gov.uk/government/publications/what-to-do-if-youre-worried-a-child-is-being-abused--2

Overview: Online Safety

Why does a school need an online safety or e-safety policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, tablets, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

"e-Safety" or online safety covers issues relating to children and young people as well as adults, and their safe use of the Internet, mobile phones, tablets and other electronic communications technologies, both in and out of school or settings. It includes education for all members of the community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. It should be noted that the use of the term 'online safety' rather than 'e-Safety' should be used to reflect the wide range of issues associated with technology and a user's access to content, contact with others and behavioural issues and is a move away from being regarded as an ICT issue.

Online safety is an essential element of all education settings safeguarding responsibilities and requires strategic oversight and ownership to be able to develop appropriate policies and procedures to protect and prepare all members of the community. The online safety agenda has shifted towards enabling children and young people to manage risk and requires a comprehensive and embedded curriculum which is adapted specifically to the needs and requirements of children and the setting. Online safety should be embedded throughout settings safeguarding practice and is clearly identified as an issue for leaders and managers to consider and address.

Schools and other educational settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating children and staff about responsible use. Schools and settings must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Whilst in some early years settings it may not feel necessary to have a separate and specific online safety policy (e.g. in small settings with no internet access for staff or children) there will still be issues regarding professional conduct, dealing

with disclosures or online abuse and data protection/security that managers and proprietors will need to consider and address. In some cases these issues can be address within other existing policies (such as health and safety, staff codes of conduct, data security and safeguarding) but managers and proprietors must ensure that they are suitably covered.

Children in all settings should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good online safety practice in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an online safety policy can and have led to civil, disciplinary and criminal action being taken against staff, children and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have and a clearly embedded and understood policy can enable education leaders and managers to ensure that safe practice is established. The online safety policy is essential in setting out how the school plans to develop and establish its approach and to identify core principles which all members of the community need to be aware of and understand.

Leaders and managers within education settings will be encouraging and supporting the positive use of Information and Communication Technology (ICT) to develop curriculum and learning opportunities as well as promoting personal enjoyment and achievements for all members of the community. It is essential that the use of ICT and online tools is carefully managed by educational settings to ensure that all members of the community are kept safe and that online risks and dangers are recognised by the setting and mitigated.

Leaders and managers within educational settings will have specific statutory responsibilities regarding ensuring and promoting children's safety and well-being which apply to both the on and offline world that today's children inhabit. Statutory government guidance which highlights this for education settings includes Keeping Children Safe in Education (May 2016 to be implemented in September 2016), Prevent and Tackling Bullying (November 2014), Screening, Searching and Confiscation (February 2014) and The Prevent Duty (July 2015).

Children and young people are likely to encounter a range of risks online highlighted as content, contact and conduct (also identified within Annex C of 'Keeping children safe in education' 2016). These issues can be summarised as:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content Child as recipient	Advertising Spam Copyright Sponsorship Hacking	Violent content Hateful Content	Pornographic content Unwelcome sexual comments	Bias Racist and extremist content Misleading info/advice Body Image and self esteem Distressing or offensive content

Contact Child as participant	Tracking Harvesting data Sharing personal information	Being bullied, harassed or stalked	Meeting strangers Sexualised bullying (including sexting) Grooming Online Child Sexual Exploitation	Self-harm and suicide Unwelcome persuasions Grooming for extremism
Conduct Child as actor	Illegal downloading Hacking Gambling Privacy Copyright	Bullying, harassing or stalking others	Creating and uploading inappropriate or illegal content (including "sexting") Unhealthy/inappropriate sexual relationships Child on child sexualised or harmful behaviour	Providing misleading information and advice Encouraging others to take risks online Sharing extremist views Problematic Internet Use or "Addiction" Plagiarism

Adapted from EU Kids Online

'Keeping children safe in education' is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Non-Maintained Special Schools (England) Regulations 2015. It applies to all schools and colleges, whether maintained, non-maintained or independent, including academies and free schools, alternative provision academies, maintained nursery schools, pupil referral units and all further education colleges and sixth-form colleges and relates to responsibilities towards children under the age of 18.

All schools and colleges must have regards to 'Keeping children safe in education' when carrying out their duties to safeguard and promote the welfare of children and schools and colleges should comply with the guidance unless exceptional circumstances arise. 'Keeping children safe in education' 2016 highlights online safety as a safeguarding issue for schools and colleges and therefore it must be considered and implemented within schools and settings statutory safeguarding responsibilities.

'Keeping children safe in education' 2016 (to be implemented in September 2016) highlights a range of specific statutory responsibilities for schools and colleges regarding online safety which governing bodies and proprietors need to be aware of. This includes (but is not limited to)the need for all staff to be aware of the role of technology within sexual and emotional abuse and also Child Sexual Exploitation and radicalisation and the need for all staff to be aware that abuse can be perpetrated by children themselves and specifically identifies sexting and cyberbullying.

The online safety (e-Safety) Policy will need to be interlinked with many different school/setting policies including the Child Protection/Safeguarding Policy, Anti-Bullying, Home School agreement, Behaviour and School Development Plan and should relate to other policies including those for personal, social and health education (PSHE) and for citizenship.

Online Safety policies will provide education settings with an essential framework to develop their online safety ethos as part of safeguarding and enable leaders and managers to set out strategic

approaches and considerations as well as ways to monitor impact. It is essential that the online safety policies are implemented as part of the settings safeguarding roles and responsibilities

Our Online Safety Ethos

Newham PRUs believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Newham PRUs identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Newham PRUs has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

Newham PRUs identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Newham PRUs online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that Newham PRUs is a safe and secure environment.
- Safeguard and protect all members of Newham PRUs community online.
- Raise awareness with all members of Newham PRUs community regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
-

This policy applies to all staff including the management committee, leadership, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, data protection and relevant curriculum policies including computing and Personal Social and Health Education (PSHE).

Online Learning Safe Use Summary

Why is ICT important?

ICT (Information and Communication Technology) across all provisions making up Newham PRUs increases the opportunities for learners to access a wide range of resources in support of the curriculum and learning. It supports the professional work of staff and enhances the management of information and business administration practice.

Access to the network and the Internet is necessary for staff and learners. It is an entitlement for all learners as it helps them to develop a responsible and mature approach to accessing information.

What are the benefits to the School? :

A number of studies and government projects have indicated the benefits to be gained through the appropriate use of ICT systems including the Internet in education.

These benefits include:

- Access to world-wide educational resources including museums and art galleries;
- Information and cultural exchanges between learners world-wide;
- News and current events;
- Cultural, social and leisure use in libraries, clubs and at home;
- Discussion with experts in many fields for learners and staff;
- Staff professional development - access to educational materials and good curriculum practice; Communication with the advisory and support services, professional associations and colleagues;
- Exchange of curriculum and administration data with the LA and DfE, using correct security procedures.

How will the School ensure Internet use provides effective learning?

- Curriculum planning will identify opportunities to enrich and extend learning activities via access to the Internet;
- Learners will be given clear objectives for Internet use;
- Learners will be provided with access to relevant and suitable Web resources;
- Learners will be informed that checks can be made on files held on the system;
- Learners using the Internet will be supervised appropriately;
- Internet access will be purchased from a supplier (such as LGfL) that provides a service designed for learners. This will include filtering appropriate to the age of learners;
- The school will work with statutory Authorities and the Internet Service Provider to ensure systems to protect learners are regularly reviewed and improved.

How will learners be taught to assess Internet content?

- ICT teaching incorporates Internet content issues, for instance the value and credibility of Web materials in relationship to other media.
- Learners will be taught to validate information before accepting it as true, and to discriminate between fact and opinion;
- When copying materials from the Web, learners will observe copyright and plagiarism rules.
- Learners will be made aware that the writer of an e-mail or the author of a Web page may not be the person claimed;
- Learners will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;

- Learners will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
- Young Learners will be encouraged to use the Internet to enhance rather than replace existing methods of research

How will Internet access be authorised?

- Internet access is a necessary part of the statutory curriculum. It is an entitlement for learners based on responsible use
- Parents will be informed that young learners will be provided with monitored Internet access.
- Learners must apply for Internet access individually, by agreeing to the Acceptable Use Policy.

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for learners. The School will supervise learners and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.

- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken

The Head Teacher working with SLT, the E-safety Co-ordinator, the Head of IT and IT technical support staff, will ensure that the policy is implemented effectively.

How will the School ensure Internet access is safe?

- All users will be informed that Internet use will be monitored
- The ICT technical leads will be responsible for checking Internet logs on a regular basis and reporting to the Head of School
- Access to the Internet logs will be restricted to senior members of staff
- Any failure of the filtering systems will be reported directly to the ICT technical team
- The School reserves the right to remove access to any website it considers inappropriate
- The School will work in partnership with parents, the statutory authorities, DFE and the Internet Service Provider to ensure systems to protect learners are reviewed and improved
- The ICT team will ensure that regular checks are made to ensure that the filtering methods selected are effective in practice
- If staff or learners discover unsuitable sites, the URL (address) and content will be reported to the network manager
- Any material that the School suspects is illegal will be referred to the appropriate authorities

The Internet is a communications medium that is freely available to any person wishing to publish a Website with no editorial intervention. While access to appropriate information should be encouraged, learners will generally need protected access to the Internet. The level of protection will be appropriate to the needs of the learner.

How will the security of the School ICT system be maintained?

- The whole system will be reviewed with regard to threats to potential threats from Internet access;
- No personal data should be sent over the Internet unless it is encrypted or otherwise secured;
- Virus protection will be installed and updated regularly;
- Personal storage devices such as USB memory sticks, MP3 players, digital cameras & mobile phones may not be used without specific permission and if required a virus check. Any unauthorised items may be confiscated, placed in a secure area and returned to the user at the end of the school day
- Devices that are taken and used away from the school will be subject to regular scrutiny to ensure that malicious applications to not breach network security systems

How will e-mail be managed?

Learners are expected to use e-mail

- Communications with persons and organisations will be managed to ensure appropriate educational use and that the good name of the School is maintained;
- Learners may send and receive e-mail as part of planned lessons;

How will publishing on the Web be managed?

- The Executive Headteacher will delegate editorial responsibility to a member of staff to ensure that content is accurate and quality of presentation is maintained;
- Web sites will comply with the School's guidelines for publications;
- Learners will be taught to publish for a wide range of audiences which might include governors, parents or young children;
- All material must be the author's own work, credit the sources used and state clearly the author's identity or status;
- The point of contact on the Web site will be the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the Web will not have full names attached and anonymity will be protected where necessary.

Social Media

Social media sites such as Facebook and Twitter will not be used by learners. Sharing of good practice through social media among professionals in education is acceptable. Staff should not authorise friend or follow requests from learners.

How will incidents be handled?

The management of the acceptable use of the Internet in school is achieved by:

- Protection software installed on the network
- Acceptable Use Policy adopted by the school
- Staff handbook containing this policy signed for by the appropriate staff
- A range of disciplinary procedures for infringements of the policy

Whenever a learner or staff member infringes the policy, the final decision on the level of sanction will be at the discretion of the School's management team

Learners: Category A infringements

- Accessing non-educational sites during lessons
- Unauthorised use of e-mail
- Use of file sharing sites on school premises.
- Transmission of commercial or advertising material

A Sanctions:

The teacher will discuss appropriate use of the Internet with the learner and the probable consequences of continued misuse. The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and the incident will be recorded in SIMS in line with the whole school behaviour policy.

Category B infringements

- Continual access to non-educational sites during lessons after being warned
- Unauthorised use of email after being warned
- Unauthorised use of social networking sites/applications, including chat rooms and newsgroups/forums.

B Sanctions:

The infringement will be brought to the attention to the Head of IT who will discuss the matter with the learner and their form tutor. There may be a telephone to the learner's parents/ carers informing them of her/ his continued misuse of the Internet. The consequences of continued misuse will be made clear to all concerned and this could include an internet ban and a detention or period in internal. The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and the incident will be recorded in SIMS in line with the whole school Behaviour policy

Category C infringements

- Accidentally accessing offensive material and not logging off or notifying a member of staff of it
- Any purchasing or ordering of items over the internet

C Sanctions:

The infringement will be brought to the attention of the Head of School or designated member of staff who will write to the learner's parents/ carers to inform them of her/ his continued misuse of the Internet and to request a meeting at which this behaviour may be addressed.

The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and s/he will face a sanction in line with the whole school behaviour policy.

The learner's use of the Internet will be closely monitored for half a term and appropriate restrictions put in place. Future use will depend on an appropriate response to the imposed sanctions.

Category D infringements

- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the School or School name into disrepute
- Deliberately corrupting or destroying others' data, violating privacy of others

D Sanctions:

The infringement will be brought to the attention of the Head of School who will write to the learner's parents/ carers to inform them of her/ his continued misuse of the Internet and to request a meeting at which this behaviour will be addressed. The learner's attention will be drawn to the *'Rules for Responsible Internet Use'* and s/he will face a sanction, in line with the whole school behaviour policy. Future access to the Internet will be at the discretion of the Head of School**Staff use of IT equipment including computers, tablets and mobile phone devices.**

The following activities will be considered a breach of the School code of staff conduct and could result in disciplinary action.

- Excessive use of Internet for personal activities not related to professional development
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998
- Bringing the school name into disrepute
- Befriending learners on personal social media accounts
- Unauthorised use of computers as per the Computer Misuse Act 1990
- Misuse of data as per the Data Protection Act 1998
- Breeching the Copyright, Designs and Patents Act (1988)

Staff are expected to undergo training as and when requested to do so by the Executive Head/Management Committee of Newham PRUs. Completion of said training is integral to maintaining the integrity of data and ensuring that all staff are aware of what constitutes acceptable use of the school's network. Non-completion of training and compliance with policy is likely to result in disciplinary action.

Mobile Phones and Media Devices

Staff will be provided with Mobile Phones if work responsibilities indicate a requirement through Health and Safety or any other aspect of individual post responsibilities deemed appropriate by the Executive Head Teacher.

Use of **Personal Mobile Phones / Mobile Device** is not permitted during contact time with students unless in exceptional / emergency situations. It is acknowledged that staff will carry personal devices throughout the school day, however personal correspondence and communications should be carried out in staff's own time and devices should be switched off / or silent during any directed contact time with students. Staff should refrain from using personal mobile phones should for personal reasons in public areas of the school building.

Employees in receipt of a **Work Mobile Phone / Mobile Device** are responsible for compliance with Data Protection Policy and also the service provider's business users contract (o2). Employees are responsible for notifying the Strategic Finance and Business Manager of any damage, theft or other problems with school-owned mobile phones or devices. Work phones should only be used for making calls or communicating with others in connection with work related matters. Mobile phones / devices must not be used for any adverse activity such as to harass someone or bring the school into disrepute. Newham PRUs or the individual provisions are not liable for any misconduct on behalf of the employee as a result of using the mobile phone or device.

The mobile device and telephone number remain the property of Newham PRUs at all times. Mobile phone handsets and telephone numbers are assigned to individuals based on identification of need,

and remain the responsibility of that person. Employees are responsible for ensuring handsets are kept safe and secure at all times and in good working order.

Mobile phone (airtime and data) usage may be monitored through the Service Contract Agreement with O2 and billing procedures. Improper usage may be recharged to individual employees.

How will staff and learners be informed?

- Rules for Internet access will be posted near computer workstations, predominantly in computer rooms.
- The Acceptable Use Policy and/or Rules for Responsible Internet Use will be printed as posters and on view around the building.
- All staff will be informed of the *Online Safety policy* and its importance will be explained.
- All staff and students will sign Acceptable Use policies and electronic copies will be retained for administration purposes.
- Parents will be informed of the *Online Safety policy* during admissions interviews and its importance will be explained. Parents will sign the student agreement and a full policy will be made available to parents on request.
- A module on responsible Internet use will be addressed in PSHE, citizenship and/or ICT lessons.

1. Introduction

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the community at Newham PRUs with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Newham PRUs.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence often associated with racist language), substance abuse, radicalisation, gang culture, gun and knife crime, racism, anti-Semitism
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming (in relation to sexual and radicalised) including CSE
- cyber-bullying in all forms

- identity theft including 'frape' (hacking Facebook profiles) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- cyber bullying / harassment
- uploading inappropriate/illegal content
- health and well-being (amount of time spent online: Internet, gambling or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film) – illegal downloading

(Ref Ofsted 2013)**Scope**

This policy applies to all members of Newham PRUs CC4 community (including staff, pupils, volunteers, parents, carers, visitors, community users) who have access to and are users of our RM CC4 ICT system, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Role	Key Responsibilities
Executive Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the provision uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular reports from the E-Safety Co-ordinator / Officer • 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)
E-Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • To liaise with the Head of IT and technical support staff • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an e-safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:

Role	Key Responsibilities
	• sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include regular reviews with the E-Safety Co-ordinator and/or Head of IT
Computing Curriculum Leader / Head of IT	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • liaises with ICT technical staff • To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • Is regularly updated in e-safety issues and legislation, and aware of the potential for serious child protection issues that can arise
Network Manager /technician	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the RM CC4 ICT system • To work with RM in maintaining data integrity across the network • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the *network / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures

Role	Key Responsibilities
	• takes day to day responsibility for data security issues
SIMS Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the provision including maintaining the LGfL USO database of access accounts
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide 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	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the *Staff Acceptable Use Policy for ICT* • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the *Student Acceptable Use Policy for ICT* • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on

Role	Key Responsibilities
	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 *Student Acceptable Use Policy for ICT* with their children • to access the provisions websites / LEARNING PLATFORM / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology •
External agencies /professionals	• Any external individual / organisation will sign an Acceptable Use Policy for ICT prior to using any equipment or the Internet within school. • Passwords for wireless access will only be distributed by IT technical support staff. • Any requests for access to specific websites for learning purposes must be made in advance to allow for manipulation of LGfL filters

Communication:

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

- Policy to be posted on the school website/Staff shared area on network
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

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

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

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

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

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

Reviewing and Monitoring Online Safety

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

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

2. Education and Curriculum

Pupil online safety or e-safety curriculum

- There is a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL e-safeguarding and e-literacy national guidance. This covers a range of skills and behaviours appropriate for age and experience, including:
- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Internet use is carefully planned to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Students will be reminded about their responsibilities through an Acceptable Use Policy which every student will sign and will be displayed throughout the school and when a student logs on to the network.
- Staff model safe and responsible behaviour in their own use of technology during lessons.
- 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;
- Staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

Newham PRUs

- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Make training available to staff on e-safety issues;
- Provide as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness

Newham PRUs

- Offers advice and guidance for parents, including:
- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information in school newsletters; on the school web site;
- suggestions for safe Internet use at home;
- provision of information about national support sites.

3. Expected Conduct and Incident management

Expected conduct

All users:

- are responsible for using the ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to the CC4 network.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the E-Safety Policy covers their actions outside as well

- will be expected to know and understand policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand policies on the taking / use of images and on cyber-bullying
- Staff
- are responsible for reading the e-safety policy and using the ICT systems accordingly, including the use of mobile phones, and any hand held or portable devices.
- Students/Pupils
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Parents/Carers
- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at the time of the admissions interview
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In Newham PRUs

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed and reported to the school's senior leaders and Governors
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- we will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law, this covers not only criminal activities such as phishing and fraud, but grooming including any incidents of sexual exploitation or radicalisation
-

- 4. Managing the ICT infrastructure

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

Newham PRUs:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
-
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment/ the London LEARNING PLATFORM/ LGfL secure platforms such as J2Bloggy, etc.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;

- Informs staff and students that that they must report any failure of the filtering systems directly to the [system administrator / teacher / person responsible for URL filtering]. Our system administrator(s) 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.

- **Network management (user access, backup)**

  Newham PRUs
  - Uses individual, audited log-ins for all users - the London USO system;
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
  - Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
  - Has additional local network auditing software installed;
  - Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
  - Storage of all data within the school will conform to the UK data protection requirements
  - Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.
  - To ensure the network is used safely, Newham PRUs:
  - Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different / use the same username and password for access to our school's network;
  - Staff access to the schools' management information system SIMS is controlled through a separate password for data security purposes;
  - We provide pupils with an individual network log-in username and they are expected to use a personal password;
  - All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform and (for older pupils) their own school approved email account;
  - We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
  - Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and also all computers automatically switch off at night to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the provision, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through CC4 Anywhere:
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- Makes clear responsibilities for the daily back up of SIMS and finance systems and other important files;

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system
- We require staff to change their passwords into the MIS, LGfL USO admin site, at least twice a year.

E-mail

Newham PRUs

- Provides staff with an email account for their professional use, London Staffmail and makes clear personal email should be through a separate account;
- Provides highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils; Uses Londonmail with students as this has email content control
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk for communication with the wider public.
-
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

Pupils:

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

Staff:

- Staff can only use the LGfL e mail systems on the school system
- Staff only use LGfL e-mail systems for professional purposes
- Access to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX;

- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;
-
- All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Newham PRUs websites

- Each provision under the Newham PRUs banner is responsible for their own website;
- The Executive Headteacher takes overall responsibility to ensure that the content of the websites is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to the website administrator authorised by the Executive Headteacher;
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the provision's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the provision's address, telephone number and we use a general email contact address, e.g. info@tunmarsh.newham.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the website;
-

Video Conferencing

Newham PRUs

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

CCTV

- CCTV is part of site surveillance for staff and student safety and for the protection of property. We will not reveal any recordings unless used as part of disciplinary action or in line with the Behaviour Policy. It will also be used where it has been disclosed to the Police as part of a criminal investigation.

5. Data security

Management Information System access and Data transfer

Strategic and operational practices

At Newham PRUs:

- The Executive Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who the key contact(s) for key information are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
- staff,
- governors,
- pupils
- parents
- This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- 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.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 5 minutes idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- 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 broadband services and the London content
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. No back-up tapes leave the site on mobile devices.

- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held.
- Portable equipment loaned for use by staff at home, where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

6. Equipment and Digital Content

Any mobile devices (either personal or owned by Newham PRUs) such as notebooks, netbooks, laptops, tablets, ipads, mobile phones, ipods, MP3 players, digital cameras, etc, can only have access to internet via any wireless system with the express permission of the SLT at the provision and this should be referred to and only actioned by the IT department.

IT support will look at the individual purpose for the use of each mobile device and decide upon the level of access to data and the shared drives on the RM CC4 Anywhere network. Maintaining data integrity is the key issue and is the responsibility of all staff, with over-riding control lying with the E-Safety coordinator and the Head of IT, working with IT support. The Executive Headteacher takes overall responsibility for e-safety provision and for data security.

Personal mobile phones and mobile devices

- Personal mobile phones are entirely at the staff member, students' & parents' or visitors own risk. The provision accepts no responsibility for the loss, theft or damage of any phone or hand held device brought in.
- Student mobile phones which are brought in must be turned off and handed in as per the behaviour policy. They are returned at the end of the day. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Executive Headteacher or the relevant member of SLT. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Executive Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Newham PRUs reserve the right to search the content of any mobile or handheld devices on the premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the 'school' telephone system. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas on site, e.g. changing rooms and toilets.

- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- We strongly advise that student mobile phones or any mobile devices should not be brought in.
- We accept that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- Any mobile device is the sole responsibility of the student.
- The Behaviour Policy states that all phones and mobile devices are handed in at the start of the day and will be securely stored. Any phone or device not handed in and found later in the day, will be confiscated and will be held in a secure place. There are consequences for these actions that are part of the Behaviour Policy. Mobile phones and devices can be released to parents or carers in such circumstances.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a 'school' phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Any permitted images or files taken with staff handheld devices, including mobile phones and personal cameras, must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.

- 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 professional duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a 'school' mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In Newham PRUs:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the agreement form at admissions interview;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published video materials / DVDs;
- Staff sign an Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- We block/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images that reveal the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all hardware are recorded in a hardware inventory.
Details of all software are 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 wiped or 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.

Newham PRUs

Acceptable Use Policy for ICT - Student Agreement

The school network has computers with Internet access to help our learning. These rules keep us safe and help us to use the computers fairly.

- I will only use the computers on the school network with permission from an adult;
- I will only login with the username assigned to me by IT support;
- I will save all my work in my own user area on the N: drive;
- I am responsible for what is on my N: drive and will report if anything should not be there;
- I will only access the websites as directed by my teacher;
- I will not access other people's files or folders;
- I will not download files without an adults permission;
- I will use computers or portable devices only for schoolwork and homework;
- I will not bring usb memory devices from outside school unless I have been given permission;
- I will only email people I know or those approved by my teacher;
- The email messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant or coercive material or messages, religious or otherwise, that are sent to me. I understand that this report would be confidential and would help protect other learners and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I understand that access to the Internet is for the purpose of learning;
- I will not use social networking sites;
- I will not attempt to bypass the school's filters;
- I will keep my password to myself;
- I will look after any portable IT devices given to me;
- Any digital content created on the school network remains the property of the school.
- I will not attempt to cause damage to any part of the school network, either by cyber-attack or by physical damage to hardware.

Signed: _____ Date: _____ (Student)

Signed: _____ Date: _____ (Teacher)

Signed: _____ Date: _____
(Headteacher/Deputy Headteacher/Head of IT**)**

Newham PRUs

Acceptable Use Policy for ICT - Staff Agreement

The rules below apply to all computers on the RM CC4 network and to any portable IT or media devices that are the property of the school and are designated for use by individual members of staff. These rules are designed to ensure that a safe ICT environment is maintained for use by all staff and pupils and ensures that the security and integrity of data is preserved.

- I will comply with all aspects of Newham PRUs ICT Code of Conduct;
- I will undergo any necessary ICT training online or otherwise for use on the Newham PRUs RM CC4 network;
- I will only use the computers on the school network for school related work;
- I will only login to the school's RM CC4 network with the username assigned to me by IT support;
- I will only login to access LGfL email with the username assigned to me by;
- I will only login to SIMS with the username assigned to me by the SIMS administrator;
- I will keep all my usernames/passwords secure and not use somebody else's to login;
- I will save my work in my own user area on the N: drive and be responsible for it;
- I will save any shared departmental work on the RMShared Documents W: drive;
- I will save any whole school documents or files on the shared RMStaff T: drive;
- I will only access appropriate websites for teaching and learning;
- I will not access other people's files unless permitted and they are on a shared drive;
- I will not download any software without referring to the IT department first;
- The email messages I send will be appropriate and for business purposes only;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not attempt to maliciously bypass the school's filters;
- I understand that any assigned portable device must be kept safe and used in a secure manner in order to not endanger the validity of data on the network;
- Any hardware or software faults with the RM CC4 network or any IT devices must be raised through the appropriate channels via IT support.

Name _____Signed: _____ Date: _____
Staff

Name _____Signed: _____ Date: _____
Line Manager

Name _____Signed: _____ Date: _____
SLT