	Name of School	**Corbets Tey School**
	Last Review Date	**19/06/2017**
	Next Review Date	**19/06/2018**
	Written by	**Susan Cumbers**
	Reviewed by	Governors Name: J Lamb Governor's Signature: 

Online Safety Policy	
Version	1.5
Date	21/11/2016
Author	online-safety coordinator (Business Manager – Susan Cumbers)

Modification History			
Version	**Date**	**Description**	**Revision Author**
1.0	12/09/2013	Initial draft	LA online-safety coordinator
1.1	11/05/15	Changes to Staff Use of Personal Devices in Equipment and Digital Content – 3rd bullet point clarification of staff contact with parents using own phones	Susan Cumbers & Emma Allen
1.2	18/05/16	Changes to staff online storage: MLE replaced with myUSO	Lisa Wellard
1.3	24/10/2016	Update to Incident Management 3rd bullet point Update to Network Management User Access Back up to include secure cloud use Cloud Environments added to p16	Lisa Wellard
1.4	21/11/2016	Update to Incident Management: Handling a sexting / nude selfie incident	Lisa Wellard
1.5	25/05/17	You Tube Filtering section added regarding the filtering level being set to 'Open'.	Susan Cumbers

Contents

Objective

The objective of this policy is to ensure that IT based policies and procedures are clearly identified, implemented and recorded to prevent misuse of Corbets Tey IT systems.

Scope (from SWGfL)

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

The term "IT" includes, but is not limited to, the following:

- personal computers (e.g. laptops and desktop PCs)
- portable and handheld devices (e.g. mobile phones, Tablets, PDAs, camera phones and cameras)
- telephone systems (mobile, landline, voicemail)
- e-mail servers, e-mail clients and all e-mail messages
- user accounts
- instant messaging
- storage media including removable media (e.g. USB memory sticks)
- software
- servers, operating systems and network devices

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying, or other online-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (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 online-safety behaviour that take place out of school.

Compliance with this policy is a condition of use of any of the schools IT systems.

Purpose

The purpose of this policy is to define the process for the control of IT systems identification of sources of risk, areas of impacts, and their potential consequences. The policy also defines the process for evaluation and decision making needed to identify the most appropriate control strategies including control and mitigation measures.

This Policy shall:

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

Risk

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

Content

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

Contact

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

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright

Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for online-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • To be responsible for ensuring that staff receive suitable training to carry out their online-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious online -safety incident. • To receive regular monitoring reports from the Online-Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal online-safety procedures(e.g. network manager)
Designated Child Protection Lead (Headteacher) Online-Safety Co-ordinator (Business Manager) Online-Safety Co-ordinator (Systems Support Assistant)	• Takes day to day responsibility for online-safety issues and has a leading role in establishing and reviewing the school online-safety policies / documents • Promotes an awareness and commitment to online-safeguarding throughout the school community • Ensures that online-safety education is embedded across the curriculum • liaises with school IT technical staff • Communicates regularly with SLT and the designated online-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • Ensures that all staff are aware of the procedures that need to be followed in the event of an online-safety incident • Ensures that an online-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 online-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: a. sharing of personal data b. access to illegal / inappropriate materials c. inappropriate on-line contact with adults / strangers d. potential or actual incidents of grooming e. online-bullying and use of social media
Governors / Online-safety governor (Julie Lamb)	• To ensure that the school follows all current online-safety advice to keep the children and staff safe • To approve the Online-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 Online-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in online-safety activities • The role of the Online-Safety Governor will include: • regular review with the Online-Safety Co-ordinator (including Online-safety incident logs, filtering / change control logs)

Role	Key Responsibilities
Computing Curriculum Leader	• To oversee the delivery of the Online-safety element of the Computing curriculum • To liaise with the Online-safety coordinator (School Business Manager) regularly
Network Manager/technician	• To report any Online-safety related issues that arises, to the Online-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school IT systems • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the school's policy on web filtering is applied and updated on a regular basis • To keep LGfL informed of issues relating to the filtering applied by the Grid • To ensure that he / she keeps up to date with the school's Online-safety policy and technical information in order to effectively carry out their Online-safety role and to inform and update others as relevant • To ensure that the use of the network / online storage (myUSO available at: https://idp3.lgfl.org.uk/idp/Authn/UserPassword) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online-Safety Co-ordinator / Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online-security and technical procedures
Online Storage	• To ensure that all data held on pupils on myUSO platform is adequately protected
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 school including maintaining the LGfL USO database of access accounts
Teachers	• To embed Online-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, 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 Online-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the Online-safety

Role	Key Responsibilities
	coordinator • To maintain an awareness of current online-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to (within their understanding) the Student / Pupil Acceptable Use Policy (NB: for many of our pupils it would be expected that parents / carers would sign on behalf of the pupils) • Have an appropriate 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 online-bullying. • To understand the importance of adopting good Online-safety practice when using digital technologies out of school and realise that the school's Online-safety policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of Online-safety policies
Teacher for Vulnerable Children and Families	• To organise and arrange parent online safety training to enable them to protect and support their children • To ensure regular online safety awareness information is distributed to parents to enable them to protect and support their children • To raise awareness of any online safety issues with parents
Parents/carers	• To support the school in promoting online-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children (if appropriate at their level of understanding) • To access the school website and to access and use other digital resources or material 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

Communication

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

- Policy to be posted on the school website/myUSO/Weekly Staff Bulletin/Shared Staff 'T' Drive
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year (where appropriate).
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in central pupil and personnel files

Handling complaints

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

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    1. Interview/counselling by teacher / teaching assistant/ Deputy/Assistant Headteacher / Online-Safety Coordinator / Headteacher;
    2. Informing parents or carers;
    3. Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
    4. Referral to LA / Police.

- Our Online-Safety Coordinator/Deputy Headteacher/Headteacher acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of online-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The Online-safety Policy is referenced from within other school policies: Computing policy, Child Protection Policy, Anti-Bullying Policy, Behaviour Policy, Personal, Social and Health Education and for Citizenship Policies.

- The school has an Online-safety coordinator who will be responsible for document ownership, review and updates.
- The Online-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online-safety policy has been written by the school Online-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders. All amendments to the school Online-safety policy will be discussed in detail with all members of teaching staff.

Version Control

As part of the maintenance involved with ensuring this policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains update information displayed on title page of the document and that all revisions are stored centrally for audit purposes. All printed versions shall be treated as uncontrolled after printing and all members of the school community should refer to school website to confirm latest version of policy.

Education and Curriculum

Pupil Online-safety curriculum

This school

- Has a clear, progressive Online-safety education programme as part of the Computing curriculum/PSHE curriculum. It is built on LA/LGfL online safeguarding and online literacy framework for EYFS to Y6/national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    1. To STOP and THINK before they CLICK
    2. To develop a range of strategies to evaluate and verify information before accepting its accuracy;
    3. 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;
    4. To know how to narrow down or refine a search;
    5. To understand how search engines work and to understand that this affects the results they see at the top of the listings [for older pupils];
    6. 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;
    7. To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    8. 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;
    9. 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;
    10. To understand why they must not post pictures or videos of others without their permission;
    11. To know not to download any files – such as music files - without permission;
    12. To have strategies for dealing with receipt of inappropriate materials;
    13. To understand why and how some people will 'groom' young people for sexual reasons [for older pupils];
    14. To understand the impact of online-bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    15. To know how to report any abuse including online-bullying; 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.

Staff should therefore:

- Plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities through an end-user Acceptable Use Policy which every parent will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and 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 / gambling;

Staff and governor training

Corbets Tey School

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on Online-safety issues and the school's Online-safety education program at staff meetings, information at weekly staff bulletins; computing events.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

The 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 online-safety behaviour are made clear
- Information leaflets; in school newsletters; on the school website;
- Updates via a regular Technology and Online Safety Newsletter:
- Demonstrations, practical sessions held at school;
- Suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.

Expected Conduct and Incident management

Expected conduct

All users

- Are responsible for using the school IT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (for many of our pupils it would be expected that parents/carers would sign on their behalf)
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online-safety practice when using digital technologies out of school and realise that the school's Online-safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on online-bullying

Staff

- Are responsible for reading the school's Online-safety policy and using the school IT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- Shall have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (within their level of understanding)

Parents/Carers

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

Incident Management

At Corbets Tey School:

- There is strict monitoring and application of the online-safety policy and a differentiated and appropriate range of 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues and online bullying incidents
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors and the LA/LSCB
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- Will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

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 Designated Child Protection Lead. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?

    - Are there any adults involved in the sharing of imagery?
    - What is the impact on the pupils involved?
    - Do the pupils involved have additional vulnerabilities?
    - Does the young person understand consent?
    - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- 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/student at the school
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 Designated Child Protection Lead 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.

Managing IT and Communication infrastructure

Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL WebScreen filtering system that incorporates Net Sweeper and Fortinet technologies, 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 (Egress Switch) to send personal data over the Internet and uses 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;
- 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 My USO 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. http://primaryschoolict.com/ and Google Safe Search
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the IT Technician/Online Safety Co-ordinator. This will be escalated to 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.

You Tube Filtering

In 2016, Google forced all YouTube traffic to be encrypted, which limited the effectiveness of safe search and keyword blocking through the WebScreen filtering service as internet filtering providers could no longer selectively filter content. As a result of these changes and to protect schools from inappropriate content LGFL servers were globally set to enforce YouTube's new restricted mode. This resulted in the school's inability to access the innocent YouTube clips that were previously accessible.

The school has therefore made a decision to change the configuration for YouTube access to 'open' which is unrestricted.

There are currently three options for filtering YouTube

- open
- moderate-restricted
- severe-restricted

The 'moderate-restricted' and 'severe-restricted' options prevent access to many innocent videos.

It is extremely important therefore that staff are vigilant in their supervision of pupils using technology and use common sense strategies in dealing with breaches of the rules of appropriate use.

We believe that the level of supervision of children and young people using the Internet and specifically YouTube will mean that all issues of access to inappropriate content will be immediately identified and dealt with in the appropriate way (See 'What we do if Guidance'). This gives our pupils an opportunity to learn about the dangers of the Internet (where appropriate and within their level of understanding) and what to do if they view anything that upsets or concerns them in a supportive and highly supervised environment. We therefore believe that in setting the YouTube filtering to 'Open' we are not restricting staff and pupils from accessing the learning content that they need during lessons but also this does create an opportunity to teach an important lesson regarding online safety in an extremely safe and supportive place.

Network management (user access, backup)

Corbets Tey School

- 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 via group policy/windows integrated server tools;
- Ensures the Online Safety Co-ordinator is up-to-date with LGfL services and policies;
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance; 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, the school:

- Ensures staff read and sign that they have understood the school's Online-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide individual usernames and passwords for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username.
- All pupils have their own unique usernames and passwords, which gives them access to the school network and 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 to email accounts;
- 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. [Users needing access to secure data are timed out after 15 minutes and have to re-enter their username and password to re-enter the network.];
- 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 we also automatically switch off all computers at 12 o'clock midnight 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 school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  e.g. Borough email or Intranet; finance system, SIMS etc.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / IT Technician; 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 pupil records; HR Administrator accesses staff records, etc.;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  e.g. teachers access a staff shared area for planning documentation via a VPN solution / RAv3 system;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support.

- Provides staff with access to content and resources through the approved online storage which staff access using their myUSO username and password;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses a stand alone CCTV system;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level;
- 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 IT 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 FMS system and administrators of the LGfL USO admin site, every 90 days.

E-mail

Corbets Tey School

- Provides staff with an email account for their professional use, LGFL Staffmail and makes clear personal email should be through a separate account;
- Provides highly restricted simulated email environments (2 Simple) for e-mail for some pupils; Uses Londonmail with students as this has email content control
- Does not publish personal e-mail addresses of pupils on the school website. Where possible we use anonymous or group e-mail addresses, for example headteacher@corbetstey.havering.sch.uk or class email addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web

Pupils

For pupils of Corbets Tey School

- 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 Computing scheme of work.
- Younger pupils are introduced to principles of e-mail through the Visual Mail or closed 'simulation' software such as 2 Simple.
- 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:
    1. 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;
    2. That an e-mail is a form of publishing where the message should be clear, short and concise;
    3. 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;
    4. They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
    5. To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    6. That they should think carefully before sending any attachments;
    7. Embedding adverts is not allowed;
    8. 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;
    9. Not to respond to malicious or threatening messages;
    10. Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    11. Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    12. That forwarding 'chain' e-mail letters is not permitted.

- Pupils (or their parents) sign the school Agreement Form to say they have understood the Online-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff

- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts is not blocked but can only be accessed during breaktimes, lunchtimes or after school;
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX and Egress Switch

- 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':
    1. the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    2. the sending of chain letters is not permitted;
    3. embedding adverts is not allowed;

- All staff sign our LA / school Agreement Form AUP to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

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

Cloud Environments

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

Social networking

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school

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

CCTV

CCTV is installed in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.
We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use them for any other purposes.

Data security: Management Information System access and Data transfer

Strategic and operational practices

For Corbets Tey School

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners in a spreadsheet named Information_asset_details.xls on the staff shared drive at:
  T:\AAA School Documents\SCHOOLPOLICIES\Other Policies\Part 1\Computing Online Safety Policies\Online Security Policy
- 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 in a spreadsheet named SingleCentralRecordCurrentStaff.xls on the shared admin drive Y:\SCR
  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  1. staff,
  2. governors,
  3. pupils
  4. 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 from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs (T Drive or Y Drive)
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 30 minutes idle time.
- We do not permit any staff to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use RAv3 with its 2-factor authentication for remote access into our systems.

- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-ups in a secure, fire-proof cabinet. No Back-ups leave the site on mobile devices.
- We use Redstor remote secure back-up for disaster recovery on our admin and curriculum server(s).
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded.

Equipment and Digital Content

Personal mobile phones and mobile devices

- Designated 'mobile use free' areas are situated in the school. The areas which are considered most vulnerable include: toilets, bathrooms and in some settings - sleep areas and changing areas.
- Mobile phones brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times.
  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 prohibited; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. 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 mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school 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.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- 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

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- 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.
- Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff members may only use their phones during school 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 permission to use their phone or keep their phone switched on at other than their break times.
    1. Teaching Assistants can request this permission from their class teachers.
    2. Class teachers can request this permission from the Headteacher and Deputy Headteacher.
    3. Admin Staff can request this permission from the Business Manager.
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited; except where it has been explicitly agreed otherwise by the Headteacher. Any permitted images or files taken in school 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.
- Staff are advised not to use their own phones for contact with parents/carers in a professional capacity. However, this is permitted in exceptional circumstances (eg: passing information to parents outside of a normal school day). All staff are advised to seek advice from senior management before sharing their personal phone numbers with parents/carers.
- 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 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.

Visitors

- All visitors to classrooms are requested to keep their phones switched off or kept switched to silent.
- All visitors must keep their phones away out of sight while on the school premises

General Rules

- **The recording, taking and sharing of images, video and audio on any mobile phone is prohibited.**
- The school has sets of still and video cameras for school staff to use within classes and on school trips.
    1. Photos and videos should be transferred to the staff shared 'T' drive on the school network on the same day as they are taken or as soon after as is reasonably possible. Any remaining data will be removed weekly from these mobile devices.
- Mobile phones brought into school are entirely at the staff member, student/parent or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

Digital images and video

Corbets Tey School will

- 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;
- 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;
- Ensure staff sign the school's Acceptable Use Policy which includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Obtain individual parental or pupil permission for the long term use any pupil photos which are used on the school website, in the prospectus or in other high profile publications;
- Block/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Ensure pupils are taught about how images can be manipulated in their Online-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;

- Advise pupils 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.
- Teach pupils that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Allow parents to take photos on personal equipment at specific whole school performances. Parents of pupils without photo permission are given the prior opportunity to withdraw their children from the performance. Parents are warned that anyone choosing to take photos or video must ensure that they do not breach the provisions of the Data Protection Act 1998 in terms of how they use the material. Any digital material can only be kept for personal use; for example to put into a family album in printed form or to keep on a personal computer or personal storage device but not placed on social media websites such as Facebook or anywhere that may be accessed more widely.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendices*:*

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Visitors)
3. Acceptable Use Agreement (Pupils)
4. Acceptable Use Agreement, Photo/video permission (Parents)
5. Protocol for responding to Online-safety incidents https://www.lgfl.net/downloads/online-safety/LGfL-OS-Policy-Infringements-July-2016.docx - handling infringements http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards
6. Search and Confiscation guidance from DfE https://www.gov.uk/government/publications/searching-screening-and-confiscation