ICT Policy

Viridis Schools

September 2022

To be reviewed in 2025 or as required

Introduction and Overview

Rationale

The purpose of this policy is to:

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

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
- Lifestyle websites promoting harmful behaviours, for example pro-anorexia/self-harm/suicide sites
- Hate content
- Content validation, for example how to check authenticity and accuracy of online content

Contact:

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

Conduct:

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (body image, internet or gaming)
- Sexting (sending and receiving of personally intimate images), also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Scope (from SWGfL)

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

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

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

Roles

- A ‘safeguarding’ culture, ensures that online safety is fully integrated with whole school safeguarding culture. The **Headteacher** has overall responsibility for online safety provision including ensuring that Governors are regularly updated on the nature and effectiveness of the school’s arrangements for online safety and ensuring school website includes relevant information.
- The **Designated Safeguarding Leads** must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance, they must ensure that staff receive suitable training to carry out their online safety roles. They will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident and ensure that an online safety incident is logged as a safeguarding incident and is kept up to date.

The **Federation Business Manager** takes overall responsibility for data and data security (SIRO) ensuring that:

- Provision follows best practice in information handling and ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements (e.g. LGfL).
- Ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager).
- Ensure that the data they manage is accurate and up-to-date.
- Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
- The school must be registered with Information Commissioner.

The ICT technician will:

- Manage the school’s computer systems, ensuring the school password policy is strictly adhered to including that users may only access the school’s networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. That systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date). That access controls/encryption exist to protect personal and sensitive information held on school-owned devices. That the school's policy on web filtering is applied and updated on a regular basis.

- Ensure the security of the school ICT system.
- 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.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network/remote access/email is regularly monitored in order that any misuse/ attempted misuse can be reported .
- That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported .
- 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.

All staff will:

- Be regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: sharing of personal data, access to illegal/inappropriate materials, inappropriate on-line contact with adults/strangers, potential or actual incidents of grooming, cyber-bullying and use of social media.
- Be aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices.
- Report any suspected misuse or problem to the Designated Safeguarding Lead or line manager.
- Maintain an awareness of current online safety issues and guidance e.g. through CPD.

All pupils will:

- Read, understand and sign e-safety agreements each year.
- 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 handheld devices.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.

All parents and carers will:

- 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 consult with the school if they have any concerns about their children's use of technology.

All of the school community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

Communication

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

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates via email, staff meetings or bulletins and training on online safety for all staff.
- Acceptable use agreements discussed with pupils at the start of each year.

Education and Curriculum

The school has a clear, progressive online safety education programme as part of the Computing curriculum/ PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience.

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

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

Parent Awareness and Training

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

- Information leaflets; in school newsletters
- Suggestions for safe Internet use at home
- Provision of information about national support sites for parents
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible

Managing the ICT Infrastructure

Internet Access, Security (Virus Protection), and Filtering

The school:

- Informs all users that internet/email use is monitored.
- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network.
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as adult content, race hate, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils.

- Ensures network health through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files.
- Uses DfE, LA or LGfL approved systems such as DFE S2S, LGfL USO FX2, Office365 secure file/email to send 'protect- level' (sensitive personal) data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes at the request of the Headteacher.
- 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 pupils.
- Requires staff to preview websites before use [where not previously viewed or cached].
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search
- Informs staff and pupil that that they must report any failure of the filtering systems directly to the IT Coordinator. Our system administrator logs or escalates as appropriate to the technical service provider or LGfL Helpdesk as necessary.
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.

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

Network management (user access, backup)

The school:

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

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school’s Online Safety & Acceptable Use Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school’s network.
- 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.
- Has set-up the network so that users cannot download executable files/programmes.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any corporate policies e.g. Borough email or Intranet; finance system, personnel system etc.
- Maintains equipment to ensure Health and Safety is followed e.g. equipment installed and checked by approved Suppliers / LA electrical engineers.
- Ensures that access to the school’s network resources from remote locations by staff is restricted and access is only through school.
- 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.
- Provides pupils and staff with access to content and resources through approved learning platforms which staff and pupils access using their username and password (their USO username and password).
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data and complies with external Audit’s requirements.
- 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.
- The wireless network has been secured to industry standard Enterprise security level/appropriate standards suitable for educational use.
- All computer equipment is installed professionally and regularly reviewed to ensure they meet health and safety standards.
- Projectors and LCD boards are maintained so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords

- 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.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use strong passwords for access into our MIS system for information on data management.
- We require staff to change their passwords into the MIS, LGfL USO admin site every 90 days when using Microsoft Office 365.
- We require staff using critical systems to use two-factor authentication when using Microsoft Office 365.
- All pupils have their own unique usernames and password which gives them access to the Internet and other services.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes. The integrated curriculum and administration networks mean 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).

Email

The school:

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

Email Retention

Mailbox users are responsible for managing their own mailbox and the data within. If you have concerns regarding the storage or deletion of an email, please contact your DPO for support.

- Emails must be automatically deleted 24 months after being received, unless required for business/critical needs or for other operational purposes.
- Email content MUST be assessed and stored in line with the Data Protection Policy.
- Devices used to store emails must meet the ICT security requirements associated with the device type. These devices must not be shared in a manner that allows unauthorised access to emails.
- When sending emails, only include the recipients necessary and are authorised to see the content. Emails must not be sent to recipients where the content is not appropriate or where there is no beneficial need or requirement.
- When forwarding emails, you are required to ensure that the recipients are correct and that the content is appropriate for said recipient.
- When replying to emails, you are required to ensure that the recipients are correct and that the content is appropriate for said recipient ensuring the tread of emails is deleted when and where appropriate.
- If you believe you have been sent an email in error, you must contact the sender immediately to confirm. This email must not be forwarded to any recipient. If the email was sent in error, it must be deleted immediately and recorded through the data breach form.
- If you send an email in error, you must attempt to recall the email in question, and then contact the recipient to inform them of the mistake and request it be deleted. You must also record this through the data breach form.

Pupils

Pupils' e-mail accounts are intentionally 'anonymised' for their protection. Pupils are introduced to and use e-mail as part of the ICT/Computing scheme of work.

Pupils can only receive external mail from, and send external mail to, addresses if the Safe Mail rules have been set to allow this. Pupils are also taught about the safety and 'etiquette' 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 or 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.

Staff

- Staff can only use the school e-mail systems on the school system and can only use these systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.
- Staff use a ‘closed’ LA email system which is used for LA communications and some ‘LA approved’ transfers of information.
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, named LA system. If there is no secure file transfer solution available for the situation, then the data/file must be protected with security encryption.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school ‘house-style’.
- The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
- The sending of chain letters is not permitted.
- Embedding adverts is not allowed.

School Website

The Communications Manager, supported by 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 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. 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.

The point of contact on the web site is the school address, telephone number and we use a general email contact address.

Cloud Environments

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

Social Networking

Staff are instructed to always keep professional and private communication separate.

Pupils taught about social networking, acceptable behaviours and how to report misuse, intimidation, or abuse through our online safety curriculum work.

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

Video Conferencing

This school uses approved or checked video conferencing sites.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation. We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Data Security: Management Information System access and Data Transfer

Strategic and operational practices

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised, i.e. the DPO.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data. Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use RAv3 / VPN solution with its 2-factor authentication for remote access into our systems.
- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL USO Auto Update, for creation of online user accounts for access to broadband services and the London content.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use Turn IT On’s NAS Discover backup for disaster recovery on our servers.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned out by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held, we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

Portable Storage Device Usage

Portable storage devices, such as external hard drives and USB sticks, are not encouraged to prevent data breaches. Staff have access to cloud storage through their school accounts and should use this to transfer or store materials.

Equipment and Digital Content

Personal Mobile Phones and Mobile Devices

Mobile phones brought into school are entirely at the staff member, students & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school. All visitors are requested to keep their phones on silent and not use the phone around the school.

The recording, taking and sharing of images, video and audio on any personal mobile phone is not permitted; except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.

Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Mobile phones will not be used unless directed by the Headteacher for specific purposes (e.g. method of contact on a school trip or site staff being contacted by contractors).

Storing, Syncing, and Access

If the device is accessed with a school owned account:

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

If the device is accessed with a personal account:

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

Pupil Use of Personal Devices

If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences;

Any device brought into school and used in breach of this policy will be confiscated.

Digital Images and Video

In this school,

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, the school will obtain individual parental or pupil permission for its long term, high profile use.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any ‘social’ online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

<u>Handling complaints</u>

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

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

- Interview/counselling by /Designated Safeguarding Lead/Headteacher
- Informing parents or carers
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework
- Referral to LA / Police.

Our school office acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of online bullying are dealt with in accordance with our Pupil Discipline and Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures. Any suspected online risk or infringement is reported to Online Safety Coordinator that day. Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

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

- Pupil Discipline and Anti-Bullying Policy
- Safeguarding and Child Protection Policy
- Social Media & Networking Policy
- Asset Disposal Policy
- FOI & Data Protection Policy
- Records Management Policy
- CCTV Policy

The Online Safety & Acceptable Use Policy has been written by the Data Protection Officer, has been reviewed by governors and is current and appropriate for its intended audience and purpose.