ICT eSafety and ICT Acceptable Use Policy

Oastlers Policy

Approved by Governing Body On	**April 2020**
To be Reviewed On	**April 2023**
Signed on Behalf of the Governing Body	**Susan Mawson**

Introduction
The use of the latest technology is actively encouraged at Oastlers School. With this comes a responsibility to protect all users and the school from abuse of the system.

It is unlikely that any set of rules can cover all circumstances that may arise. The following set of rules is not intended to be a complete list of all possible "offences". The emphasis is on outlining standards of performance and behaviour which are expected of Oastlers Staff and any users of Oastlers ICT Services.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed, as such the use of certain technologies have been restricted for the safety of staff and learners. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Oastlers School we understand the responsibility to educate our learners on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for school's to use technology to benefit learners.
Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.
Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and learners) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, ipads, mobile devices,

webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by learners and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring
Our IT support, Primary Technology or members of Senior Leadership Team may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask to speak to the Headteacher.

Primary Technology or members of Senior Leadership Team may monitor, intercept, access, inspect, record and disclose emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under General Data Protection Regulation (EU) 2016/679 (GDPR), or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by Primary Technology staff and comply with the GDPR 2016, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Oastlers subscribes to Bradford Learning Network which provides a service to help with the safeguarding children on the internet with centrally managed firewalls; as well as Smoothwall which provides firewalls and internet filtering at a local level. Along with BLN we subscribe to e-Safe which is able to and report nuances in vocabulary related to safeguarding risks, allowing us to intervene quickly.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches
A breach or suspected breach of policy by a school employee, contractor or learner may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Learners who breache the policy shall be dealt with in line with the Behaviour Policy.

For staff any policy breach could be grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner’s powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the GDPR 2016.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's business manager. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Business Manager and Headteacher.

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Acceptable Use Agreement: Learners

- I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes
- I will not download or install software on school technologies
- I will only log on to the school network, other systems and resources with my own user name and password
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address (if I have been provided one)
- I will make sure that all ICT communications with learners, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone I do not know from the internet
- I am aware that when I take images of learners and/ or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, learners or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day
- I will not sign up to online services until I am old enough to do so

Acceptable Use Agreement: Staff, Governors and Visitors
Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct
ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with IT Manager.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with learners and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to learners
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of IT Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of learners and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help learners to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches and mobile phones) in the school between the hours of 8.30am and 3.30pm.
- I understand this forms part of the terms and conditions set out in my contract of employment

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school
Signature …….…… Date ……
Full Name ……..... (printed)
Job title ……

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- All ICT equipment must be connected to the school network regularly to make provision for anti-virus updates
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the Business Manager immediately. The Business Manager will advise you what actions to take and be responsible for advising others that need to know.

Data Security

General Data Protection Responsibilities: key responsibilities for School Heads and Governors

- The accessing and appropriate use of school data is taken very seriously, as such the school have outlined the below procedures that staff must abide by.
- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used
- Anyone sending a confidential or sensitive email should use secure packages such as Galexkey.

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response. Previously called a Senior Information Risk Officer (SIRO), the Headteacher has the following responsibilities:

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

Disposal of ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
- The disposal of all ICT equipment should be fully compliant with requirements of GDPR regulations.
- Disposal of any ICT equipment will conform to:
    - The Waste Electrical and Electronic Equipment Regulations 2006
    - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

  General Data Protection Regulation 2016
  https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
    - Date item disposed of
    - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
    - How it was disposed of e.g. waste, gift, sale
    - Name of person & / or organisation who received the disposed item

** if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed*.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
The Waste Electrical and Electronic Equipment Regulations 2006
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website

https://ico.org.uk/

General Data Protection Regulation 2016

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

PC Disposal – SITSS Information

http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

Email

The use of email within Oastlers school is an essential means of communication for both staff and learners. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or learner based, within school or international. We recognise that learners need to understand how to style an email in relation to their age and how to behave responsible online.

Staff and governors should use a school email account for all official communication to ensure that learners are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing email

- The school gives all staff & governors their own email account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- Staff & governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact learners, parents or conduct any school business using personal email addresses or personal equipment
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending emails to external organisations, parents or learners are advised to cc. the Headteacher, line manager or designated line manager
- Learners may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
  - Delete all emails of short-term value
  - Organise email into folders and carry out frequent house-keeping on all folders and archives
- All learner email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments
- Learners must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email
- Staff must inform (Primary Technology or Business Manager) if they receive an

offensive email
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply

Sending emails
- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, should be marked as such and sent through protected email source such as Galexkey.
- Use your own school email account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School email is not to be used for personal advertising

Receiving emails
- Check your email regularly
- Activate your 'out-of-office' notification when away for extended periods (if you do not know how, training can be provided by the IT Manager on request)
- Never open attachments from an untrusted source; consult the IT Manager first
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of emails is not allowed

Emailing Personal or Confidential Information
- Where your conclusion is that email must be used to transmit such data obtain express consent from your manager to provide the information by email and <u>exercise caution when sending the email and always follow these checks before releasing the email:</u>
  - Encrypt and password protect. See Business Manager for instructions
  - Verify the details, including accurate email address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to email requests for information
  - Do not copy or forward the email to any more recipients than is absolutely necessary
  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an email
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any email
  - Request confirmation of safe receipt

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is the Headteacher. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and learners, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: safeguarding, health and safety and behaviour (including the anti-bullying) policy and PSHCE.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the learners on a regular and meaningful basis.

- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating learners about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Learners are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Learners are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Learners are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Learners are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff
- Members of staff or an organisation such as Childline or the 'CEOP report abuse'
- Teachers can access 'Teaching online safety in school' (DfE,2019c) for further guidance about keeping children safe online.
- Learners will receive regular whole school input during assemblies to ensure that they are kept up to date with all current issues with regard to their safety when they are on line.

eSafety Expectations for Staff

- All members of staff will ensure that they are aware of e-safety issues affecting staff, parents/carers and learners. Keep up-to-date through our ICT Lead, CEOP and SID (Safer Internet Day) or other CPD events.
- Staff will remind learners of key e-safety messages such as 'never give out personal details online', be aware of your digital footprint
- I will report any accidental access to inappropriate material to the IT Manager immediately
- I will report any inappropriate websites to the Business Manager
- Staff will be vigilant when searching for images and asking learners to search for images and encourage use of creative commons and royalty free image sites

- If a learner accesses inappropriate material staff will report it following the correct procedures
- If I suspect a safeguarding issue I will report it to the Designated Safeguarding Lead and follow the correct procedures.
- I will always be myself and will not pretend to be anyone or anything that I am not on the Internet.
- I will always protect the online reputation of the school and act in a digitally professional way

eSafety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see eSafety Coordinator)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the learners at the start of each school year
- eSafety posters will be prominently displayed
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities, whole school assemblies and so on

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported Primary Technology or Business Manager

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the Headteacher.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator or Business manager.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for

very serious offences in line with our Safeguarding Policy and Staff Code of Conduct or in the case of learners to dealt with in accordance to the behaviour policy

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the Oastlers network is filtered through the Smoothwall and monitored by eSafe Global.

Whenever any inappropriate use is detected it will be followed up and acted upon appropriately.

Managing the Internet

- The school provides learners with supervised access to Internet resources (where reasonable) through the school's intranet.
- The school's internet provision is filtered through the Smoothwall and any inappropriate keyword searches are flagged via e-Safe Global to the Business Manager.
- In appropriate use of the internet may result in a timed ban.
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with learners
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/Careers recheck these sites and supervise this work. Parents/Careers will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, learners, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and learners and how this is disseminated.

Infrastructure

- Our school also employs some additional web-filtering (local smoothwall web filter and Impero) which is the responsibility of the Business Manager in consultation with Primary Technology.
- Oastlers School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; GDPR 2016, Regulation of

Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and learners are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow learners access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or learners discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the Primary Technology staff to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Learners and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the Primary Technology staff to install or maintain virus protection on personal systems. If learners wish to bring in work on removable media it must be given to the Primary Technology staff for a safety check first
- Learners and staff are not permitted to download programs or files on school based technologies without seeking prior permission from Primary Technology.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed immediately.

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our learners to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The school Primary Technology controls access to social networking, messaging and blogging sites. All have been blocked unless requested by staff to be use for educational purpose.
- All learners are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Learners are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Learners are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our learners are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Learners are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our learners are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate

with learners using the school learning platform or other systems approved by the Headteacher

- When signing up to online services that require the uploading of what could be deemed as personal or sensitive data, schools should check terms and conditions regarding the location of storage.
  Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

Passwords and Password Security
Passwords
Password security is essential for staff, particularly as they are able to access and use learner data. Staff are expected to have secure passwords which are not shared with anyone. The learners are expected to keep their passwords private and not to share with others, particularly their friends. Staff and learners are regularly reminded of the need for password security:

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised Primary Technology staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a learner or colleague your password**
- **If you aware of a breach of security with your password or account inform the Business Manager or Primary Technology staff immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and learners who have left the school are removed from the system within one week

If you think your password may have been compromised or someone else has become aware of your password report this to the Business Manager or Primary Technology staff.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email, learning platform and Management Information System (subject to requirement) log-in username. From the first successful logon they are also expected to use a personal password and keep it private
- Learners are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform,

including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- In our school, all ICT password policies are the responsibility of the Business Manager and all staff and learners are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to all users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorised access

Personal or Sensitive Information

Protecting Personal or Sensitive Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal or sensitive information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal or sensitive information contained in documents you fax, copy, scan or print. This is particularly important when shared MFD's (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal or sensitive information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal or Sensitive Information Using Removable Media

- Only use school encrypted removable media.
- Store all removable media securely
- Return to the Business Manager when the removable media is no longer need, this will then be securely deleted to comply with GDPR 2016
- Encrypt all files containing personal or sensitive data (see page 19)
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all access information such as web addresses, logon IDs and PINs confidential and do not disclose them to anyone
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. Guidance can be found here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

- With the written consent of parents (on behalf of learners) and staff, the school permits the appropriate taking of images by staff and learners with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of learners, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Learners are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of learners, staff and others at any time.
- Learners and staff must have permission from the Headteacher before any image can be uploaded for publication

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Learner's Images and Work

On entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the

press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Learners' names will not be published alongside their image and vice versa. Email and postal addresses of learners will not be published. Learners' full names will not be published.

Before posting learners work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Headteacher has authority to upload to the internet.

Storage of Images

- Images/ films of learners are stored on the school's network and backup server
- Learners and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and learners within the confines of the school network or other online school resource
- The Business Manager has the responsibility of deleting the images when they are no longer required, or when the learner has left the school

Webcams and Surveillance Cameras

Please refer to the schools Data Protection Policy including Data Management and CCTV for further guidance

- The school uses surveillance cameras for security and safety. The only people with access to this are the Headteacher and Business Manager. Notification of camera use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- We may use CCTV Images and footage for the purposes of training and supporting staff development
- CCTV Images and footage will be used, where appropriate, in allegations management. This may also be shared with other agencies where applicable.
- Any viewing of recorded images must be compliant with regulations required by the **Information Commissioner's Office** (ICO)
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)
    - Webcams can be found IT Suite, staff notebooks and school iMacs. Notification is given in this/these area(s) filmed by webcams by signage
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- Oastlers school log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- All staff must ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to the Buissness Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and General Data Protection Regulations 2016
-

Portable & Mobile ICT Equipment

This section covers such items as laptops, ipads, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with this and all other policy's referenced in this policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the

Business Manager, fully licensed and only carried out by the Primary Technology staff
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- Using own/private mobile devices for personal conversations (including texting and other forms of social media communication) or use for personal business purposes (non-urgent appointments, etc). This restriction applies during teaching time, peripatetic lessons, directed time, social events during the school day, trips and visits, assemblies or other whole school events or meetings/training of any kind
- Staff must not use their own personal mobile number to contact parents and carers unless it is exceptional circumstances with the permission of the Headteacher and personal numbers are withheld.
- Learners are allowed to bring personal mobile devices/phones to school but must leave them in reception throughout the school day. At all times the device must be switched onto silent
- The school is not responsible for the loss, damage or theft of any personal mobile device
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Telephone Services

- School telephones are provided specifically for school business purposes and personal usage is not allowed unless it is an emergency
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call

may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that you are available to take any pre-planned incoming telephone calls
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. For clarification on this please see the business manager

Servers
- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- System backups should be encrypted by appropriate software
- Data must be backed up regularly
- Back up media stored off-site must be secure

Social Media, including Facebook and Twitter
Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.
- Staff **are not** permitted to access their personal social media accounts using school equipment at any time, unless prior approval is given by the Headteacher
- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach learners the safe and responsible use of Social Media
- Staff, governors, learners, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, learners, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, learners, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

Systems and Access
- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Review Procedure

There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety issue that concerns them

There will be on-going opportunities for staff to discuss with a member of SLT any issue of data security that concerns them

This policy will be reviewed every (24) months and consideration will be given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

This policy has been read, amended and approved by the staff, head teacher and governors.

Further help and support

Oastlers School has a legal obligation to protect sensitive information under the GDPR 2016.. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

Advice on eSafety – www.nen.gov.uk/e-safety

School's toolkit is available - Record Management Society website – http://www.rms-gb.org.uk/resources/848

Test your online safety skills http://www.getsafeonline.org

Information Commissioner's Office – www.ico.org.uk

Cloud (Educational Apps) Software Services and GDPR 2016 – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2015. This is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their

obligations and duties in relation to the GDPR 2016, particularly when considering moving some or all of their software services to internet-based "cloud" service provision – https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

Current Legislation

Acts Relating to Monitoring of Staff email

General Data Protection Regulations 2016

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their Safeguarding packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

GDPR 2016

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services