ICT Acceptable Use & Online Safety Protocols

Published: August 2019

Review: July 2020

Contents

ICT Acceptable Use Protocols: All Staff within Ilketshall St Lawrence School

All staff employed by Ilketshall St Lawrence School or working on behalf of Ilketshall St Lawrence School, who are working with ICT equipment must ensure that they have read, understood and signed the ***ICT Acceptable Use Agreement*** which incorporates by reference, these protocols and the ***ASSET Trust Wide 'GDPR guidelines for Staff'***

It is expected that ICT systems in the schools will be used mainly for educational purposes, and school use should always have priority over personal use.

These protocols cover the use of any school owned devices and any personal devices when they are being used by staff for school business or activities. Devices include laptops, PCs, tablets, iPads, smartphones or similar e.g. Smartwatches.

Use of the Internet and E-mail for School Business or School-Related Activities

1. All use of the Internet at school should be primarily to enhance teaching and learning or for administrative use, although it is understood that staff may occasionally need to use the Internet for personal reasons.

2. All users should be expected to adhere to the generally accepted rules of network etiquette, as follows:

   - Remember the professional/personal divide in your ICT use.
   - Be polite and use appropriate language in your messages to others.
   - Do not use language that could be considered defamatory, obscene, menacing, illegal, or that could be calculated to incite hatred against any group.
   - Do not reveal the address, telephone number, e-mail or other personal details of other users, and think very carefully before revealing your own details.

3. Use of e-mail

   - Personal data (see *glossary* and *ASSET GDPR Policy* for definition) must not be emailed beyond the school network. A secure file transfer or web download needs to be activated when sending data to approved third parties.

     Agreements must be in place before personal data is shared – you must seek the assistance of the Systems and IT Manager or ASSET data controller if you need to send personal data.

   - E-mails to external individuals or organisations should be written carefully, following the rules of network etiquette outlined in (2). All school e-mails are disclosable information under the Freedom of Information Act and must be seen by staff as a formal school communication that is in the public domain.

   - E-mails/messages from parents are likely to come in to the **admin@ilketshallstlawrenceprimary.co.uk** address or through the **SeeSaw or Tapestry Learning Journal**. Any reply from a member of staff through their own email account will mean that the parent will then have the staff e-mail address. If the e-mail/message covers any major issues or principles, then the message should be shared with SLT and the opinion of the SLT should be considered before replying. In such occurrences, a formal letter or email may need to be sent. If email is used, the email address used should be the one above.
   - Significant e-mail responses to parents should have the text submitted to a member of SLT for checking prior to being sent – staff should use their professional judgement, but if there is any doubt consult a member of SLT. When the e-mail is sent, a copy should be copied to the SLT. If the incident is related to Safeguarding, a copy of the email should be submitted to MyConcern.

- Should staff start receiving inappropriate e-mails, or find that parents/others are using their e-mail as a direct line of communication that is unwanted, they should inform the most appropriate member of SLT, and ensure they keep the email(s) and print out a hardcopy.

- The contact details on the website should be the school address, e-mail (school or one specific to blog, forum or wiki) and telephone number. Staff or pupils' personal information should not be published.

Use of ICT hardware and software

1. Each member of staff has a unique login for the network. Passwords must not be given to other staff or pupils. The passwords should be changed regularly, but not during school holiday periods. Staff should avoid obvious ones; more secure passwords usually include a combination of letters, numbers, upper and lower case letters and even symbols.

2. When using laptops or devices with pupils, staff are expected to be in the room at all times and are responsible for ensuring, as far as possible, that use of the facilities by pupils is appropriate.

3. All software installed on teacher devices supplied by Ilketshall must have a valid licence for that use. It is also vital to remember that music files, films and eBooks etc. are covered by copyright and that staff must not infringe this legislation – the rules covering personal use and school use in this area are often different – there is separate guidance on this issue you can find online.

4. School equipment needs to remain secure at all times to be covered by insurance and not left in cars or other vulnerable places as these may not be covered by insurance.

5. All devices supplied for teachers are provided for professional use and it is the responsibility of staff to ensure their devices are not used inappropriately by others.

6. Pupils must not be allowed to use staff laptops, devices or staff PCs in the classrooms or offices, unless under close supervision, e.g. when making a presentation to the rest of the class.

7. Use of personal devices on the school network needs to be agreed with your technician or the IT Manager (iPads, tablets, smartphones or other peripherals) before accessing the school network.

Child Protection

1. Safeguarding children is of paramount importance and ICT protocols need to be mindful of this. Pupils and parents sign a permission agreement for using the Internet. If a photograph is used anywhere on the website or in blogs, forums or wikis, this should be done in accordance with the Photo Permission form. Use general captions e.g., working in the science lab, or first names only.

2. If a pupil name is used in full in the text of a publication, avoid using their photograph.

3. If a photograph is likely to be used again, make sure that it will be stored in a secure place on the school network.

4. Whilst access to unsuitable Internet content is minimized by filtering software, this can never be completely eliminated. It is therefore important that staff be vigilant to prevent as much as possible pupils and other staff accessing or searching for inappropriate website content.

5. Staff must not use their mobile phones or other personal devices to take pictures of pupils. Photo permission information must always be checked and followed – information is available on Scholarpack or from School Office.

6. All photographs taken by staff of pupils and by pupils of staff, need to be of a professional nature and taken in line with the photo permission form submitted by parents/carers.

7. It is the responsibility of all staff of Ilketshall St Lawrence School to promote online safety (see guidance on online safety or your Online Safety Lead if you are unsure) for all pupils, students and staff.

Data Storage

1. Staff are responsible for regularly reviewing the data on their personal network area. Files which are no longer used and duplicate files must be deleted from the drive at the earliest opportunity.

2. Staff should not store non work-related files (photographs, music etc.) on the school network. Only material with a specific educational purpose should be stored on the school network.

Parent / Carer Acceptable Use Agreement

All parents and carers are asked to sign the acceptable use of IT policy regarding the school and these are highlighted below. If a member of staff feels that any of these have been broken by a parent, please inform a member of the SLT.

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that the school and members of staff are protected against defamatory statements online.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

Online Safety

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- *regular meetings with the Online Safety Lead*
- *regular monitoring of online safety incident logs*
- *reporting to Governors at meetings*

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and Online Safety Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Online Safety Lead will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead:

- Works alongside Designated Safeguarding Lead in taking day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Plans the Online Safety teaching units within the Computing curriculum
- Liaises with the Local Authority / Academy Trust
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors
- Reports regularly to Headteacher

Technical staff:

The Technical Staff /Online Safety Lead is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that the use of the network, email and internet is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher; Online Safety Lead for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead:

Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming

- cyber-bullying

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school

Policy Statements

Education of pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing / PSHE / other lessons and should be regularly revisited
- Key Online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- All staff will be required to sign the online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

Training – Governors

Governors should take part in Online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / Academy Trust or other relevant organisation.

- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- The "master / administrator" passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Executive Principal/Headteacher or other nominated senior leader and kept in a secure place
- The IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
  There is a clear process in place to deal with requests for filtering changes.
- Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- AUA is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of online safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

□ The school has a set of clear expectations and responsibilities for all users

□ The school adheres to the Data Protection Act principles

□ All users are provided with and accept the Acceptable Use Agreement

□ All network systems are secure and access for users is differentiated

- Where possible these devices will be covered by the school’s normal filtering systems, while being used on the premises All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Glossary

Personal data includes names, addresses, dates of birth, photographs, SEND information, external exam results and so on

Sensitive and High Risk Personal Data - Sensitive personal data is defined in the DPA as information concerning an individual’s:

- racial or ethnic origin
- political opinions

- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual orientation
- criminal convictions or alleged offences

Links to policies mentioned in this document:

ASSET Social Media Policy (1),

KS1 Acceptable Use Agreement (2),

KS2 Acceptable Use Agreement (3),

Staff Acceptable Use Policy (4), - Available upon request from the school

ASSET GDPR Policy