# ICT (including E-Safety & Acceptable Use) Policies
## (see also Social Networking Policy)

## 1. Introduction

Information and Communication Technology (ICT) has an extremely important role to play in the development of young people for their future in the 21st Century. The continuous and fast moving developments in technology are affecting everyone's working and social life. It is vital that the use of ICT within Lealands High School reflects these changes across the whole of its curriculum and administration support system.

E-safety encompasses not only internet safety but also the safe and appropriate use of electronic devices such as mobile phones and wireless technology. E-safety focuses on educating children and young people about the benefits, risks and responsibilities of using information technology. Our E-safety procedures provide safeguards and raise awareness to enable users to control their online experiences.

## 2. Responsibility

This policy has been drawn up to protect all parties – the pupils, the staff and the school. The school system is primarily for business use and this policy applies to all school employees and other users who have agreed and signed this policy.

ICT developments are planned by the Senior Leadership Team and in particular the Assistant Headteacher responsible for ICT. Staff have the opportunity to contribute to the strategy. Overall responsibility for e-safety lies with the Headteacher and school Governors.

## 3. Broad Goals

- To enable all pupils and staff safe access to ICT and the internet.
- To promote the safe use of new technologies.
- To facilitate the use of new technologies as a learning tool which enhance pupils' experiences in all areas of work and the curriculum.

### 3.1 Investment

Following significant investment in 2008 as part of the BSF project, the school is now committed to continued investment to allow refurbishment of aging hardware as part of a rolling programme throughout the school. This allows us to keep up with future developments within the curriculum and keep pupils best prepared for the future. The school will maintain and develop its current level of expertise and use of ICT through the staged introduction of new hardware and infrastructure and a continual monitoring of both hardware and software developments in order to inform future purchases. These developments will include a regular review of staff CPD.

The school will work in close partnership with partner organisations such as Luton Futures, the Local Authority and School Support Service @ Luton and well as other external support providers. All ICT hardware and software is the property of the school and not of an individual member of staff, faculty or department and may be relocated in order to gain the maximum benefits from it.

## 4. Application

4.1 Access to School Networks and externally hosted sites

All pupils and staff have access to the school's Curriculum Network and cloud based storage and email through Google Apps for Education, staff also have access to the Administration Network, the shared structure within the Google Drive and the SIMS Management Information System. Teachers also have access to a number of secure hosted sites which hold information about pupils such as Show My Homework, Class Charts and SISRA. Access to all networks, Google Apps for Education, SIMS and other external sites are controlled by passwords which are required to be at a high level of complexity (e.g. passwords must contain a minimum of eight letters and must include some capitals and at least 2 numbers). All staff are advised to keep passwords secure and are required to change their network and email passwords termly. School IT security systems including virus protections are reviewed regularly.

Rules governing the use of the school's networks are made known to all users. All users are required to agree to the IT Acceptable Use Policy (AUP). Records are kept to ensure that staff have signed the policy. The school reserves the right to take appropriate action in the event of a user breaking the rules. Visitors to the school who wish to connect to the internet via the visitor network are made known about, and required to agree to, relevant aspects of the AUP.

4.2 Legal Responsibilities

The school accepts its responsibilities in respect of:

- compliance with the Data Protection Act;
- access to the Internet;
- software licences;
- The Misuse of Computers Act.

## 5. Security & E-Safety

5.1 The Internet

The internet is an essential element in 21st century life for education, business and social interaction. The school understands its duty to provide pupils and staff with quality internet access as part of their learning experience. The use of the internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

The school has in place systems which safeguard users and reduce the risks that can occur in the use of the internet. These include:

- the school internet being designed for pupil use and including filtering and monitoring solutions appropriate to the age of pupils;
- pupils being taught the correct uses of the internet as well as what uses are inappropriate and being given clear guidance for good internet use;
- pupils being educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation;
- pupils being shown how to publish and present information to a wider audience, how to evaluate internet content and how the use of this content has to comply with copyright law;
- pupils being taught the importance of cross checking information before accepting its accuracy;
- the school controlling access to social networking sites, and educating pupils in their safe use outside of school;
- pupils being advised never to give out personal details of any kind which may identify them, their friends or their location;

- pupils and parents being advised that the use of social network spaces outside school brings a range of dangers;
- pupils and parents being taught about the dangers and implications of all forms of cyber bullying;
- pupils being advised to use nicknames and aliases if using social networking sites outside of school;
- procedures for staff or pupils who come across unsuitable online materials, the site being reported to the Assistant Headteacher with responsibility for ICT and/or the Manager of IT and Network Services who will ensure it is blocked in school;
- all staff being given the school ICT policy (including e-safety) and its importance explained;
- all staff reading and signing the school ICT Acceptable Use Policy for staff before using any school ICT resource or connecting to any networks;
- all pupils reading and agreeing to the school IT Acceptable Use Policy for pupils which is introduced through Computing lessons and integrated as part of the taught curriculum;
- parents' and carers' attention being drawn to the school ICT policy (including e-safety) and IT Acceptable Use Policy for pupils through newsletters, and on the school website;
- the school maintaining a current record of all staff and pupils who are granted access to school ICT systems;
- the school asking all new parents to sign the parent/pupil agreement when they register their child with the school;
- staff and pupils being aware that the storage of personal or inappropriate files on their school network area is not appropriate (as per the IT Acceptable Use Policy for pupils);
- staff and pupils being informed that network and internet traffic and network use can be monitored and traced to the individual user.

5.2 E-mail

The use of email is an important element in the running of the school, and both staff and pupils have access to the email system. There are a number of safeguards in place to ensure that the system remains secure and safe for all users. These include:

- pupils being able to access their Google Apps email account within school as a sole means of email communication;
- pupils only being able to send and receive emails to and from other members of the school community using their school email; pupils being required to immediately tell a teacher or another member of staff if they receive offensive e-mail;
- the safe and effective use of email being integrated into the KS3 Computing curriculum;
- in email communication, pupils being told that they must not reveal their personal details or those of others, or arrange to meet anyone without specific permission;
- incoming email being treated as suspicious and attachments not opened unless the author is known;
- staff and pupils being informed that the use of the school email system should be restricted to matters relating to school;
- staff and pupils being informed that email activity which could be construed as cyber bullying will be dealt with in line with the school bullying policy;
- staff and pupils being informed that email content can be monitored and traced to the individual user.

5.3 Workflow

A number of additional solutions to support workflow and organisation are in place within the school to support communication between staff, pupils and parents. As of November 2016 these include Google Classroom, Show My Homework and Class Charts. These solutions are subject to the same conditions as for the use of the school network, internet provision and email as set out above and as set out in the IT Acceptable Use Policy for pupils.

5.4 School Website

The school website is used to provide information to a range of audiences; especially parents/carers. It is important that the information on the website is up-to-date and accurate. All staff have a responsibility to ensure that information related to areas for which they hold responsibility in school is up-to-date and accurate. The Marketing & Communications Administrator maintains the website under the direction of the Business Manager. The Head's PA can also add urgent information to the website as authorised by the Headteacher or Deputy Headteacher. Safeguards are in place to protect pupils and the reputation of the school which are:

- staff or pupils personal contact information not being generally published. The school contact details being given online should only be the school office;
- pupil photos should not include first and surnames together to identify individuals with their own photographs;
- the Headteacher taking overall editorial responsibility and ensuring that content is accurate and appropriate;
- the ICT policy (including e-safety) should be available on the website along with other key school policies.

5.5 Video conferencing & new technologies

The use of new technologies is something that the school is keen to develop for pupil use and is essential to learning in the 21st century. There are a number of safeguards in place to ensure that the use of technology remains secure and safe for all users. These include:

- video conferencing using the school network to ensure quality of service and security;
- emerging technologies being examined for educational benefit before use in school is allowed;
- the senior leadership team noting that technologies such as mobile phones with wireless internet access (outside the school's managed network) can bypass school filtering systems and present a new route to undesirable material and communications;
- mobile phones not being used by pupils while on the school site;
- the sending of abusive or inappropriate text messages or files by Bluetooth, BBM or any other means being forbidden;
- the use by pupils of cameras in mobile phones being forbidden;
- the uploading of unauthorised videos/images by staff or pupils onto the internet (e.g. YouTube, Facebook) being forbidden.

5.6 Externally published material including photographs

There are many times in school where photographs are taken of events and individuals in order to create a record of school life and for use in internal documentation. There are a number of safeguards for the use of photographs and personal information including:

- written permission from parents or carers will be obtained before photographs of pupils are published (e.g. on the school website, in prospectuses etc.);
- work is only published with the permission of the pupil and parents/carers;

- pupil image filenames do not refer to the pupil by name;
- parents are clearly informed of the school policy on image taking and publishing.

5.7 Pupil data and personal information

All data on laptops and other means of data storage that leave the school building should be encrypted if individual pupils can be identified. Staff are made aware about the importance of confidentiality of personal information and data about staff and pupils.

As part of the induction pack for new pupils, parents/carers are given the document ‘Privacy Notice – Data Protection Act’ which provides them with our procedures regarding the use of pupil data and signposts them to websites where they can find out more information.

5.8 Introducing e-safety to pupils

Through the wider curriculum and explicitly in Computing lessons pupils are taught about e-safety and given clear guidance for safe use of ICT. E-safety posters are posted in all rooms and discussed with pupils. All pupils are informed that network and internet use will be monitored and appropriately followed up.

5.9 Handling e-safety complaints

Complaints of internet and other misuse must be reported to the Assistant Headteacher with responsibility for ICT and/or the Manager of IT and Network Services and will be dealt with accordingly.

- All e-safety incidents are recorded by the Manager of IT and Network Services.
- Any complaint about staff misuse must be referred to the Assistant Headteacher in charge of ICT and the Headteacher.
- Any complaints regarding cyber bullying must be dealt with in accordance with the school bullying policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents are informed of the complaints procedure (see school’s complaints policy).
- Pupils and parents are informed of consequences for pupils misusing the internet.

## 6. Acceptable Use of Mobile Devices (including Laptops)

6.1 The use of laptops and other mobile devices which are issued by the school

Staff who are allocated a school laptop or other mobile device must adhere to the school’s Acceptable Use Policy and Mobile Device Loan Agreement. The policy and agreement requires that:

- the device should only be used by the person to whom it has been issued;
- when in school, devices should not be left unattended and should be kept secure at all times;
- when out of school, devices should not be left unattended in vehicles and should be kept safe and secure;
- the device should only be used for purposes relating to school;
- data should be stored securely in line with the Data Protection Act;
- all data on laptops and other means of data storage that leave the school building should be encrypted if personal information relating to staff or pupils can be identified;
- data available via the Google Drive or email system can be accessed using the device but users need to make every effort to keep access to these secure;
- staff are made aware about the importance of confidentiality of personal information and data about staff and pupils;

- photographs, videos and personal data should not be stored on the device;
- personal files should not be stored on the device;
- public networks should be used cautiously and securely;
- staff are informed that all network and device use can be monitored and traced to the individual user;
- installing, copying, allocating, or using software which violates copyright, intellectual property rights or software licensing agreements is forbidden;
- all software must be installed/approved by the schools IT Department and not by the member of staff to whom the device was issued;
- modifying the Operating System, software or hardware configurations without permission is prohibited;
- if you believe the mobile device has been hacked or infected with a virus, you should power the device off and contact the schools IT support team immediately;
- food and drink is kept safely away from the equipment;
- care is taken when carrying the device;
- if taken out of school, the device should be covered by the allocated users home insurance policy;
- the device should be made available to the IT support team periodically for a health check;
- damage to a device should be reported to the IT support team as soon as possible after the damage occurs;

6.2 The use of mobile devices which are not owned by the school

Pupils are not permitted to use their own mobile devices in school.

Staff who wish to use their own mobile devices in school are able to do so but should be aware that:

- devices should be kept secure by the owner and any damage or loss are the responsibility of the owner;
- devices used on the school site should be used for school purposes;
- photographs, videos and data relating to school should not be stored on these devices;
- information available via the Google Apps for Education or Email system can be accessed using the device but users must ensure that this is keep secure;
- school wireless networks are accessible and this can be arranged with the agreement of the Manager of IT and Network Services;
- staff are informed that, when using the school network, device use can be monitored and traced to the individual user.

## 7. Disposal of IT Equipment & Data

Disposal of redundant IT equipment is the responsibility of the school's IT support team. No equipment will be disposed of until the school's IT support team have checked it.

- At the time of disposal, the school's IT support team will take possession of the equipment and record this against the school's IT inventory and asset disposal form. All data must be removed and backed up if required (to optical media or the network).
- The school's IT support team is responsible for identifying a suitable disposal route; normally this is through registered organisations that forward equipment onto charities, negating most environmental and liability issues.
- All disk drives must be securely erased either using software that wipes out unused space on all disks completely by securely overwriting data on the physical level using [One Pass Zeros] data destruction method as a bare minimum.

- If there is a contractual agreement with a company who takes responsibility for the disposing/recycling of the IT equipment, a certificate of data destruction is required.
- In certain situations where a physical drive is faulty or not working, the drive must be destroyed using whatever means possible ensuring the data is not recoverable; this must then be disposed of in compliance with WEEE.

## 8. The Computing Department

The Assistant Headteacher with responsibility for ICT will oversee this area of the school as part of the SLT link system.

The Subject Leader for Computing has responsibility for:

- attainment, leadership, curriculum, teaching and behaviour in Key Stage 3 and Key Stage 4 Computing;
- developing, monitoring and evaluating the provision of Computing to ensure access for all pupils to their entitlement in relation to the National Curriculum;
- monitoring pupil progress in line with the school assessment policy;
- coordinating intervention and support as necessary for pupils who are not making the expected progress in Computing and ICT;
- marking at both key stages; to ensure portfolios of evidence are built on for Key Stage 3 and Key Stage 4 to ensure success;
- carrying out other duties/responsibilities not specified above following reasonable discussion and negotiation with the Linked Assistant Headteacher.

## 9. Teaching & Learning

The educational experiences and teaching and learning styles used within the school must reflect the use of ICT in the outside working environment and the changing needs of both staff and pupils. Every opportunity is sought to enhance curriculum delivery and pupils work in general through the use of ICT.

9.1 To achieve this, the school believes that:

- all staff and pupils should have access to ICT resources to support their work;
- Subject Leaders should, with the assistance of the Assistant Headteacher with responsibility for ICT, ensure that ICT is embedded into every subject across the curriculum;
- the use of ICT within the curriculum should involve a range of activities such as:
    - ➢ the use of Microsoft Office applications
    - ➢ access to information sources such as the internet for research purposes
    - ➢ specialist subject software in all subject areas
    - ➢ communications such as email
    - ➢ cloud based storage of files via the Google Apps for Education Drive
    - ➢ work flow solutions such as the use of Google Classroom
    - ➢ ICT being used as a teaching aid by staff
    - ➢ the use of a range of platforms and devices
- provision should be made for hardware, software and support materials to assist pupils with special educational needs, and EAL.

9.2 All pupils and staff should:

- have access to ICT facilities during the school's opening hours within the school year;
- have their existing skills recognised and the opportunity to further develop these skills through the CPD training programme;
- be able to access Google Apps for Education for cloud storage and email use as defined above at all times;

9.3 The school will ensure that all pupils regardless of ability will:

- have an ICT entitlement;
- have the opportunity to use ICT appropriately across the curriculum;
- develop autonomous use of ICT equipment;
- develop skills, knowledge, ideas and concepts with regard to ICT in a progressive manner.

## 10. Maximum Use & Further Developments

To ensure that the school makes maximum use of its ICT facilities and continues to develop its potential:

- computing will be taught as a discrete subject in Years 7, 8 and 9;
- ICT and Computing courses will be available as an option in Years 10 and 11;
- cross curricular provision will be co-ordinated by the Assistant Headteacher in charge of ICT;
- pupils will be able to use the ICT facilities available during other lessons, if there is space, by using a booking system;
- staff may use ICT facilities when they are not teaching;
- staff will be expected to have a minimum standard of ICT competency;
- staff will be able to access training related to their individual needs;
- staff competency in ICT will be monitored and continue to be developed through staff CPD;
- highly skilled ICT-competent teachers will be encouraged to assist other staff as well as further develop their own skills, which includes training opportunities.
- all teaching staff will be issued with a computer or laptop for use in school and out of school where appropriate.

## 11. Monitoring, Evaluation & Review

This policy will be reviewed annually by the Assistant Headteacher with responsibility for ICT and will be presented to the School Governing Body on an annual basis for ratification.

The items within this policy will be monitored, evaluated and reviewed through the AEP, DEF and DEAP for Computing, and the AEP for Whole School ICT

The Headteacher has overall responsibility for the successful implementation of this policy. This policy should be read in conjunction with our Social Networking Policy.

## 12. Related Policies

The following policies should be read in conjunction with the ICT (including E-Safety) Policy:

- IT Acceptable Use Policy (Staff)
- IT Acceptable Use Policy (Pupils)
- Social Networking Policy

Lealands
High School

# IT Acceptable Use Policy (Pupils)

All pupils must follow the conditions described in this policy when using the school IT network, email and other solutions provided by the school.

Breaking these conditions may lead to:

- withdrawal of the pupil's access;
- close monitoring of the pupil's network, internet and email activity;
- investigation of the pupil's past network, internet and email activity;
- in some cases, criminal prosecution.

School staff will regularly monitor the network to make sure that it is being used responsibly. The school will not be responsible for any loss of data as a result of the system or mistakes in using the system by the user.

**Conditions of Use**

Student access to the networked resources is a privilege, not a right. Students will be expected to use the resources for the educational purposes for which they are provided. It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Policy. Pupils must also accept personal responsibility for reporting any misuse of the network to a member of staff.

**Acceptable Use**

Students are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All use, however, should be consistent with the school ethos and code of conduct. The following list does provide some examples that must be followed:

- only use ICT systems in school, including the internet and email, for school purposes;
- do not download or install software on school equipment;
- only log on to the school network, other systems and resources with your own username and password;
- do not reveal my passwords to anyone and change them regularly;
- only use the school email account for anything related to school;
- make sure that all ICT communications with other pupils, teachers or others in the school community is responsible and sensible;
- be responsible for my behaviour when using the Internet including the sites and resources that you access and the language that you use;
- do not browse, download, upload or forward material that could be considered offensive or illegal. If you accidentally come across any such material report it immediately to my teacher;
- do not give out any personal information such as name, phone number or address;
- do not use your own mobile devices including mobile phones, ipads and laptops within school;
- support the school approach to online safety and do not upload or add any images, video, sounds or text that could upset any member of the school community.

I understand that all my use of the network, internet, email 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 will be contacted.

Lealands
High School

# IT Acceptable Use Policy (Staff)

The use of ICT and 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 the Assistant Headteacher with responsibility for ICT.

**Acceptable Use**

All staff are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All use, however, should be consistent with the school ethos and code of conduct. More information about acceptable use is contained within the ICT (including E-Safety) Policy and the Social Networking Policy. The following statements form an agreement for staff about the acceptable use of ICT:

- I will only use ICT equipment provided by the school for professional purposes relating to my role or for uses deemed acceptable as agreed by the Headteacher or Governing Body.
- I will ensure that any devices provided by the school will be used in a way that is consistent with the guidance set out in the mobile device loan agreement.
- I will only use the school network, internet provision, SIMS, Google Apps for Education and other products provided by the school a for professional purposes relating to my role or for uses deemed acceptable as agreed by the Headteacher or Governing Body.
- I will not disclose any passwords provided to me by the school or other related authorities.
- I will not use the username and password of any other members of the school community.
- I will ensure that all electronic communications with pupils 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 pupils.
- I will only use the approved, school email system for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without the permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils 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.
- I will support the schools 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 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.
- If using my own device for school purposes I will ensure that I adhere to the above as appropriate.

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:** | **Job Title:** |