Lincoln Minster School

Acceptable Usage of ICT - Pupils

1. **Policy Statement**

In line with the common mission of United Learning, the use of ICT at Lincoln Minster School is primarily about learning and is about improving our pupils' opportunities in education through the use of established and emergent technology to enhance learning outcomes.

We are committed to ensuring that this mission is the shared responsibility of all those who contribute to the use of ICT across the school, including those with strategic responsibility, those providing teaching and learning support, and those with network planning and technical support roles. Thus, it is intended that ICT is used where appropriate:

- to enhance the learning experience of our pupils
- to facilitate best teaching practice by teachers
- to improve effectiveness, achieve efficiencies and promote best practices in administrative systems.

To support our mission, Lincoln Minster School has a number of policies and procedures in place to guide and support those who utilise ICT. Both pupils and teachers have access to computer resources, e-learning material and a learning platform. The ICT is driven by sophisticated Local Area Networks (LAN) and the Best in Everyone (BiE) Net Wide Area Network (WAN) that ensure safe, secure and timely access to e-mail, e-learning resources, printing, the Internet and educational software. However, we are mindful that technological safeguards go hand-in hand with promotion of best practice, responsible and appropriate usage and so our ICT policy and procedures documents are intended to promote positive outlook and behaviour regarding responsible ICT usage and Internet safety.

It is the responsibility of every staff member, both teaching and non-teaching, to ensure that the spirit of the policies set out below is implemented across all relevant areas of learning, teaching, administration and support:

- Acceptable usage policy document for ICT for STAFF
- Acceptable usage policy document for ICT for PUPILS (KS3/KS4 and KS5)

This policy applies to all members of our school community, including boarders and those in our EYFS setting.

Lincoln Minster School is committed to ensuring that the application of this policy is nondiscriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Treatment Policy.

Lincoln Minster School seeks to implement this policy through adherence to the procedures set out in the rest of this document.

In line with our Provision of Information policy, this document is available to all interested parties on request from the main school offices and should be read in conjunction with the following policies: Academic Integrity, Anti-Bullying, Controlled Assessment (B), Behaviour, Curriculum, Equal Opportunities, Health and Safety, Mobile Phones, Child Protection (Safeguarding).

This document is reviewed annually by the IT Manager or as legislation change requires.

Reviewed By	George Kellow; IT Manager
Approved By	Lee Crew; DFO
Review Date	September 2025
Reason for Change	Annual Review
Next review date	September 2026

Lincoln Minster School
An education for life

United Learning
The best in everyone™

Contents

1. Policy Statement	***Page 1***
2. Key Personnel	***Page 4***
3. Introduction	***Page 4***
4. Educational ICT Vision	***Page 4***
5. E-Safety	***Page 5***
6. Use of the Internet	***Page 6 -7***
6.1 Internet Use in the Boarding Houses	***Page 6***
7. Use of Emails	***Page 7***
8. Use of Social Media, Internet Messaging and Chat Rooms	***Page 7 - 8***
8.1 Risks	***Page 7 8.2***
Implementation	***Page 8***
9. Cyber Bullying	***Page 8 – 10***
9.1 Text Messaging	***Page 9 9.2***
Instant Messaging and Chat Rooms	***Page 9 9.3***
Websites	***Page 9***
10. Copyright and Plagiarism	***Page 10***
11. Use of Personal Laptops on the School Network	***Page 11***
12. Use of Personal Storage Devices	***Page 11***
13. Data Security	***Page 11***
14. Health and Safety	***Page 12***
14.1 Regulations	***Page 12***
14.2 Ergonomics	***Page 12***
14.3 Working Environment	***Page 12***
15. How to Report Misuse or Accidental Access of Inappropriate Materials	***Page 12***
16. Monitoring by the School	***Page 13***
17. Sanctions for Misuse	***Page 13 - 14***
17.1 Legal Implications	***Page 13***
17.2 Local Enforcement	***Page 13***

Appendix 1: **Policy on the Acceptable Use of ICT Facilities by Pupils** ***Page 15***
Appendix 2: **Policy on the Acceptable Use of the Internet by Boarding Pupils** ***Page 19***
Appendix 3: E**xemplar letter detailing action taken when pupil ICT policy infringed** **Page 20**

2. Introduction

The use of Information and Communications Technology (ICT) at Lincoln Minster School is about learning, especially e-learning. It is about improving children's life chances in education through the use of established and emergent technology to enhance learning outcomes. It is about academic results, certainly, and the tangible results that show improved breadth as well as depth of achievement. But it is also about those activities and experiences that enhance leadership and teamwork. In this sense, the Communications element of ICT sometimes takes precedence over the Information element. The use of interactive communications technology can enhance those attributes that are valued by further and higher education as well as by employers and parents. However, the use of ICT brings with it new concerns about attitudes and values. It is our task to ensure that these attitudes and values evolve to maximise pupils' opportunities to evolve into responsible citizens. Adherence to the common mission of United Learning is one of the tests that must be applied to the use of ICT at Lincoln Minster School. Clear goals for the use of ICT are spelt out in our school vision – both formally within the School Development Plan, and less formally via the articulation and reiteration by leadership at all levels. ICT is not implemented as a result of the efforts of one department alone, but it is a whole-school effort. Underpinning all of these is an ethos in which our shared values and beliefs are reflected.

ICT is used successfully at Lincoln Minster School as a result of a climate conducive to success. This is a consequence of the involving, and sharing responsibility to, all those who contribute to the use of ICT across the institution, from those with strategic responsibility, teaching and learning support, network planning and technical support. The physical environment and resources to support this must also be in place. Systematic network migrations and upgrades have helped improve ICT infrastructure, and schools, academies and central office continually work together to ensure that the resources are in place for curriculum and administration delivery. It is important that policies are in place to guide and support those who utilise ICT.

Positive outlook and behaviour is promoted through a number of these policies, including sections on responsible ICT usage and Internet safety. Technological safeguards go hand-in hand with promotion of best practice, responsible and appropriate usage.

In the implementation of ICT to support e-learning, there is a commitment to raising standards. It must never be forgotten that ICT in education is about learning and teaching.

3. Educational ICT Vision

Lincoln Minster School has a curriculum that is designed to specifically reflect national and local aspirations, career and Higher Education opportunities and the skills and talents required in the community. ICT installed in our school reflects this curriculum, as well as providing technological tools to enhance high-quality teaching and learning. Every classroom has an interactive flat panel display (IFPD) or interactive whiteboard and a data projector connected to a computer allowing the preparation and delivery of dynamic, interactive lessons across all curriculum areas. Internet facilities are available in learning spaces and every teacher and student has an email address and access to materials that allows collaboration and home access to teaching and learning materials.

Both students and teachers have access to computer resources, e-learning material and a learning platform. The ICT is driven by sophisticated Local Area Networks (LAN) that ensure safe, secure and timely access to e-mail, e-learning resources, printing, the Internet and educational software.

Other facilities within our school includes computerised administration systems as well as specialised equipment used for specific subject areas. The curriculum is supported by the learning and teaching resources provided, which include up-to-date ICT facilities. High quality professional development ensures that teachers are amongst the best trained ICT practitioners in the country. Appropriate interactive whiteboard training is offered to staff. This training, along with ICT resourcing combines with exciting and innovative teaching practices to help ensure that pupils enjoy the best learning experience possible, giving them the skills and the knowledge necessary for success in the 21st century. The Central Office ICT and e-Learning team supports the development of our specific educational ICT vision policy. It is the responsibility of the Head Teacher to satisfy themselves that policies are in place that adequately reflect the ethos and curriculum of the school as well as informing practice. It is the responsibility of every staff member, both teaching and non-teaching, to ensure that the spirit of the policies is implemented across all relevant areas of learning, teaching, administration and support.

The use of ICT within Lincoln Minster School to support learning, teaching and administration is not an optional extra to be avoided. Neither is it to be used indiscriminately. ICT should be used where appropriate to enhance the learning experience of pupils and to facilitate best teaching practice by teachers. Administrative systems must be used to improve effectiveness, achieve efficiencies and promote best practice. Line managers will have responsibility to ensure that ICT usage achieves all of the above.

4. E-safety

Safe use of the internet and e-mail is important to both teachers and parents. Lincoln Minster School provides student access to the internet and other services. Consequently, we have systems in place to ensure that pupils use the technology safely, access only appropriate materials, and protect both themselves and school facilities from possible risks. Lincoln Minster School use CEOP, and other associated online safety materials, to deliver safety awareness lessons to pupils. Regular training and awareness of internet safety issues is delivered to parents by CEOP trainers. Teachers at Lincoln Minster School also receive training and updates on the importance of internet safety. The Assistant Head: Pastoral and Designated Safeguarding Lead is also trained directly by CEOP.

Lincoln Minster School endeavours to always balance the desirability of fully exploiting the vast educational potential of internet resources for learning and communication with safeguards against the risks and unacceptable activity. The Acceptable Use Policy is signed by pupils as acceptance of the terms by which the school provides access and so forming a 'contract' for ICT use. The acceptable usage policy is firmly embedded within the school ICT development plan.

E-safety is taught within the PSE programme delivered by Form Tutors. Discrete e-safety themes, appropriate to age group, are taught in PSE in each year group of the senior school. It is essential that

e-safety is embedded and integrated within broader PSE topics in order that an appropriate context is set (for example, teaching the topic of sexting within the wider issues of self-esteem, respect and sexual attitudes).

The following policy guidelines are based on an important Ofsted report on the use of ICT in schools: ***The safe use of new technologies***. The focus of the report was 'to evaluate the extent to which schools teach pupils to adopt safe and responsible practices in using new technologies'.

In the interpretation of the findings from the report, the following action has been taken:

- **Internet filtering**. The use of 'managed' systems to develop e-safe behaviour in preference to 'locked down' access.
- **Curriculum**. e-safety is embedded within the curriculum in the Prep and Senior schools
- **Staff training and engagement.** High quality training tailored to meet the needs of the teacher or staff user - rather than 'one size fits all'. Staff training audits, including admin support staff are regularly carried out.
- **Policy.** Policy is regularly reviewed in order to be appropriate to context
- **Beyond the school gate.** Regular communication with parents and carers is facilitated by the use of Parent Mail and the school website. Parents also have individual log-in details to the learning platform. Parents are given an annual opportunity to attend an evening of e-safety awareness delivered by CEOP Ambassadors.

ICT policies are reviewed and updated at regular intervals. The Assistant Head, (Teaching and Learning) is responsible for leading and coordinating review process.

5. Use of the Internet

Pupils at Lincoln Minster School have good access to computer resources. The computers work across a network and allow safe, secure and quick access to different electronic resources, printing, educational software and high-speed Internet access. Pupil use of the Internet is clearly laid out in the pupil copy of the Acceptable Use Policy (see Appendix 1). It is a requirement that each pupil reads, agrees and signs a copy of the policy before they are allowed to use the Internet in school. This process is administered by Form Tutors annually and the form sets of signed copies of the pupil declaration are kept in the main school office.

The pupil AUP includes the following statements specifically related to pupil use of the Internet:

- You do not access the Internet for inappropriate purposes.
- You do not use the Internet if it is not directly related to your school work.
- You do not use strong language, swearing or aggressive behaviour when using the internet or other digital communication devices.
- You do not type anything on a website that might be offensive.
- You do not force your viewpoint on to others. It is important to be polite at all times.

- You do not give personal information (for example, address or phone number) to anyone on the internet.
- You agree to the school viewing with just reason and without notice any e-mails you send or receive, material you store on the school's computers, or logs of websites you have visited.
- You do not download information from the internet without identifying where the information came from (for example, Source: www.bbc.co.uk).

Failure to adhere to the pupil AUP will lead to one or more sanctions as laid out in 13. Sanctions.

5.1 Internet use in the boarding houses

There are additional e-safety rules governing the use of the Internet in the boarding houses. These are included in Appendix 2. These e-Safety rules help to protect boarding pupils and Lincoln Minster School by describing acceptable and unacceptable computer use. They complement the existing whole school ICT policy. However, a signed acknowledgement of an awareness of this boarding policy has been signed by the pupil and parents/guardian(s) and is held by the housemaster/mistress responsible for each house (filed within the pupil's personal documents).

As a result of infrastructural challenges, internet access in Eastgate House boarding house is now provided by an appliance managed and maintained by the school IT Services department. This is a separate system that makes use of hardware and software outside the normal school computer network. Internet access is wireless and when the necessary written permissions have been received, pupils are provided with an internet connection. The devices are handed to the House parents, who enter the confidential security key to access the wireless signal in each device. The details of the security key are kept confidential and are greyed out by default.

The Mount and Hillside boarding houses have wireless internet access provided as an extension of the school network. As such it is monitored and maintained in the same fashion as the main school network (wired and wireless).

The school IT team is responsible for the security settings of each of these devices. The devices provide a good range of administrative controls and these are appropriately applied and managed by the school IT team.

This is a deliberate policy decision in order to allow a customisation and tailoring of Internet access to need – to include, for example, Skype, social networking sites and webmail.

6. Use of E-mails

Pupils each have a school email address as part of our Microsoft Office 365 offering. Senior school pupils receive specific advice as to the use of e-mail and the appropriateness of language used. The advice forms part of the wider e-safety awareness delivered in school by ICT and Form Teachers. Use of e-mail is covered by the pupil Acceptable Use Policy (Appendix 1).

7. Use of Social Media, Internet Messaging and Chat Rooms

So-called Web 2.0 social software such as Facebook and Twitter are providing opportunities for personal expression, the creation of communities, collaboration and sharing. Other examples include blogs (personal web-based journals), moblogs (blogs sent from a mobile phone), wikis (modifiable collaborative web pages), and podcasting (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). They enhance or gain value from social interactions and behaviour. They can also provide opportunities for collective intelligence and thus add value to data. Digital video, photography and music technologies have democratised the process of content creation and distribution.

Recent studies of children and young people's online behavior indicate that there are a wide range of activities undertaken, from using the internet for homework and research to a wide range of entertainment and edutainment activities. The benefits for children are well documented, but so too are a number of risks of which young people must be made aware.

7.1 Risks

Initial concern for children was largely centered on their use of social networking sites and the possibility that young people could be 'groomed' by those with a malicious intent. This is made possible by the amount of personal information that children can disclose online allowing predators to manipulate children by becoming their online friend, often hiding their true age and identity and developing close friendships by pretending to share common interests in music, personalities, sport or other activities for which children have expressed a specific liking. The huge publicity surrounding chat rooms and the decision by some leading commercial companies to close their chat rooms to children led to the focus switching to social networking applications. In some respects these are more of a problem than chat rooms, as young people share 'friend lists' and pass on contacts one to another. As instant messaging programs allow private one to one correspondence with or without the use of webcams, they also can give even greater privacy to predators developing relationships with children online.

It is important to understand that social networking sites are public spaces where adults can also interact with children, which obviously has an implication on child safety. Whilst encouraging young people to be creative users of the internet who publish content rather than being passive consumers, there is a balance to be weighed in terms of the personal element of what is being published. The concerns are shifting from what children are 'downloading' in terms of content to what they are 'uploading' to the net. In some cases very detailed accounts of their personal lives, contact information, daily routines, photographs and videos are acting as an online shopping catalogue for those who would seek children to exploit, either sexually or for identity fraud purposes. These sites are very popular with young people as not only can they express themselves with an online personality, but they can use all the applications the site has to offer to chat and share multimedia content with others - music, photos and video clips. Unfortunately, these sites can also be the ideal platform for facilitating bullying, slander and humiliation of others. The better sites are now taking this issue seriously and ensuring that they have safety guidelines and codes of practice in place.

7.2 Implementation

A majority of Social Networking sites are not allowed in school and are blocked by the web filtering software. Additional privileges are given to boarders using networked computers in school, for example there is less restrictive filtering of some social networking sites - but keeping in line with the overall ethos of providing a safe environment (for example, web mail accounts are accessible after normal school hours). The management of mobile devices and laptop dongles that allow unrestricted access in dormitories is carefully managed. Within the boarding environment, restrictions are more local and managed by the Head of Boarding as identified above.

In summary, the Lincoln Minster whole school policy towards Social Networking sites is:

- Use CEOP materials to educate children about risks and benefits
- Only use social networking sites that safely enhance education experiences e.g. It's Learning
- Social networking sites are by default blocked by web filtering software – and remain restricted until reviewed by an appropriate staff member
- Provide timely and accurate information for parents/guardians and teachers e.g. CEOP awareness evenings to parents/guardians
- Provide safety tips and good advice
- Stay up to date on developments e.g. via the United Learning Group ICT Newsletter

8. Cyber-bullying

With increasing new communication technologies being made available to children and young people, there will always be a potential for them becoming a victim to online bullying. Online bullying, ebullying or cyberbullying, is defined as follows: 'the use of information and communication technologies such as email, [mobile] phone and text messages, instant messaging, defamatory personal websites and defamatory personal polling websites, to support deliberate, repeated, and hostile behaviour by an individual or a group, that is intended to harm others.'

Children and young people are keen adopters of new technologies, but this can also leave them open to the threat of online bullying. An awareness of the issues and knowledge of methods for dealing with online bullying can help reduce the risks.

8.1 Text Messaging

Bullying by text message has become an unfortunate and unpleasant by-product of the convenience that SMS (short message service) offers. Children are advised to be careful about giving out their mobile phone number, and ask that those that have their number never pass it on. If only known and trusted friends know the number, it is less likely to be abused in this way. If being bullied by text message, children should immediately seek help from a teacher, parent/guardian or carer. They should not respond to the messages, but should keep a detailed diary recording information such as the content of the message, the date, the time, the caller ID or whether the number was withheld or not available. If space permits, the messages should also be stored on the phone in case they are needed later as evidence. Abuse in the form of bullying should be reported to the mobile phone company who can take certain steps to try to resolve the situation, and in some instances it may also be necessary to

involve the police. In some cases it may be necessary, or easier, to change the mobile phone number or to purchase a new phone.

Like bullying by text message, email provides a reasonably 'anonymous' method of communication which bullies have seized upon to harass their victims. If being bullied by email, children should not respond to the messages, but should seek help from a teacher, parent/guardian or carer. Likewise if they receive an email message from an unknown sender, they should exercise caution over opening it, or ask an adult for assistance. Don't delete the message but keep it as evidence of bullying. If the email is being sent from a personal email account, abuse should be reported to the sender's email service provider. Many email programs also provide facilities to block email from certain senders. If the bullying emails continue, and the email address of the sender is not obvious, then it may be possible to track the address using special software. Email service providers may be able to offer assistance in doing this. In certain cases, it may be easier to change the email address, and exercise caution over who this new address is given to.

8.2 Instant Messaging and Chat Rooms

Aside from the general risks of using chat rooms and instant messaging (IM) services, these services are also used by bullies. Children should be encouraged to always use moderated chat rooms, and to never give out personal information while chatting. If bullying does occur, they should not respond to messages, but should leave the chat room, and seek advice from a teacher, parent/guardian or carer. If using a moderated chat room, the system moderators should also be informed, giving as much detail as possible, so that they can take appropriate action.

Instant Messaging (IM) is a form of online chat but is private between two, or more, people. If a child is bullied or harassed by IM, the service provider should be informed giving the nickname or ID, date, time and details of the problem. The service provider will then take appropriate action which could involve a warning or disconnection from the IM service. If a child has experienced bullying in this way, it might also be worth re-registering for instant messaging with a new user ID.

8.3 Websites

Although less common, bullying via websites is now becoming an issue. Such bullying generally takes the form of websites that mock, torment, harass or are otherwise offensive, often aimed at an individual or group of people. If a child discovers a bullying website referring to them, they should immediate seek help from a teacher, parent/guardian or carer. Pages should be copied and printed from the website concerned for evidence, and the internet service provider (ISP) responsible for hosting the site should be contacted immediately. The ISP can take steps to find out who posted the site, and request that it is removed. Many ISPs will outline their procedures for dealing with reported abuse in an acceptable use policy (AUP) which can be found on their website. Additionally, many websites and forum services now provide facilities for visitors to create online votes and polls, which

have been used by bullies to humiliate and embarrass their fellow pupils. Again, any misuse of such services should be reported to a teacher, parent/guardian or carer who should then take steps to contact the hosting website and request the removal of the poll.

Specific issues regarding online bullying are dealt with by the school's existing anti-bullying policy.

Cyber-bullying is included as a distinct section within the Pupil Acceptable Use Policy (Appendix 1).

The pupil AUP includes the following statements specifically related to pupil use of the Internet:

1. You do not use mobile phones, including sending or receiving text messages, during the normal school day. KS5 pupils are allowed to use their mobile phones within the confines of the sixth-form common room during school hours.
2. You do not use strong language, swearing or aggressive behaviour when using the internet or other digital communication devices.
3. You do not type anything on a website or send an e-mail that might be offensive.
4. You do not force your viewpoint on to others. It is important to be polite at all times.
5. You do not give personal information (for example, address or phone number) to anyone on the internet or by e-mail.

9. Copyright and Plagiarism

The school abides by copyright legislation if the intention is to use or publish materials through the internet. The use of online materials for teaching and learning is different from the use of printed and television or audio broadcast materials, which are covered by the and the Educational Recording Agency (ERA).

All materials published on the web (irrespective of format) are subject to copyright law and may not be copied or otherwise reproduced without the copyright owner's permission. Permission may be granted by the owner as stated at their site, or it may need to be obtained directly from the owner. It is insufficient just to acknowledge the source.

Just because something is published on the Web it does not automatically fall into the public domain. If Internet materials are clearly labelled as being copyright-free or in the public domain then it may be legally acceptable to use the materials.

Similar care should be used in copying music, video or other materials from CDs, CDROMs or DVDs. Possession of the originals does not automatically entitle the user to copy the contents in any format and may be illegal unless expressly authorized on the media or packaging itself.

The school participates in the auditing of copyright usage and works with the CLA to collect reliable data to use in their surveying process. The last CLA survey was undertaken between 11/01/12 and 27/03/12.

Plagiarism is included as a distinct section within the Pupil Acceptable Use Policy (Appendix 1). The pupil AUP includes the following statements specifically related to plagiarism:

- You do not download information from the internet without identifying where the information came from (for example, Source: www.bbc.co.uk).
- You do not use another's disk, including a USB Memory Stick, as if it were your own work, or copy work belonging to someone else and use it as if it were your own.
- You do not use someone else's artwork, pictures or graphics (including graphs, spreadsheets and so on) as if they were made by you.

10. Use of Personal Laptops on the School Network

Lincoln Minster School does not support nor allow any use of personal laptops on the fixed school network. Personal laptops may be used in school but will not work across the fixed school network. There is no technical support provided for personal laptops, including those owned by staff and pupils. Requests for technical support, including the configuration of personal laptops to work across the school network, will be declined.

There is a provision for wireless internet access across via the school wireless network. This is filtered and monitored through the school filtering systems. Usage of this system is governed by the rules of the School Network Usage Policy. Any unauthorised or inappropriate usage will be traced back to a user account and the owner of that account will be held accountable.

Where a need is identified, the school may issue a school laptop. A school laptop will be configured to run on the school network and will also work independently. Use of the school laptop is covered by the terms of reference contained within this policy document.

11. Use of Personal Storage Devices

Historically portable USB storage devices have provided staff and students with a cost-effective method of saving, storing and transporting data between home and school. They are simple to use and can normally be used with any computer or laptop and the alternatives were either unreliable, more insecure or expensive to implement. However, USB storage devices do bring significant issues:

- Devices can fail, and files/data lost without any backup; people become reliant on them as the only location to store data
- Devices are easy to lose or misplace
- It is easy to store sensitive data on the devices in breach of data protection rules. Even encrypted USB devices pose risks of data loss if the devices fail or are misplaced
- It is easy to infect school networks with viruses residing on the USB devices
- The files are not accessible on mobile devices without USB ports

The implementation of Office365 to schools, and the cloud storage it brings, means that these devices are no longer needed to store or transport data. As such the use of USB storage devices on the school network is disabled and such devices are not authorised for use on school systems.

Further information can be found in the USB Portable Storage Device Policy.

12. Data security

Information held on the school's computer systems may only be accessed with proper authorisation and if the information is pertinent to school work. Under no circumstances should personal or other confidential information held on computer be disclosed to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computer Misuse Act 1990. At Lincoln Minster School we store data on a network drive where it is regularly backed up. Any mobile storage devices such as USB pen drives or external hard disks that contain sensitive or pupil data are appropriately encrypted.

Passwords protect school systems from access by unauthorised people. Therefore network and VLE passwords should never be given or shared with another pupil. Procedures are in place on systems to ensure users change passwords on a regular basis, passwords are of a minimum length and old passwords cannot be reused immediately. It is recommended that passwords are six or more characters long and include at least one numeric or non-alphabetic special character. The connection of non-corporate computer equipment to the network without prior written request and technical approval is forbidden. This includes connection via dialup or Virtual Private Networking (VPN).

13. Health and Safety

Most ICT-related health and safety issues are dealt with under the under the Health and Safety policy as outlined in the school's Safety Compliance File. Updated guidance on the Health and Safety (Display Screen Equipment) Regulations 1992 as amended by the Health and Safety (Miscellaneous Amendments) Regulations 2002 was published in 2003. The Regulations cover all display screen equipment used by employees but the majority of requirements apply only to those employees who can be defined as "users".

13.1 Regulations

- The use of display screen equipment by pupils is covered by this policy and all workstations at which school members work comply with the minimum requirements;
- An assessment is carried out by Health and Safety representatives on each workstation and this is recorded. The assessment is carried out to cover the workstation itself (display screen plus furniture), the environment and the interface between the computer and user. This assessment is carried out using the VDU workstation checklist available from www.hsebooks.co.uk;
- Once an assessment has been carried out, any remedial action, as indicated by the checklist is taken. Assessments are regularly reviewed;

- The regulations and new guidance set out requirements for workstations etc. and assessors are recommended to obtain a copy (via HSE Books) ISBN 0-7176-25852-6;

13.2 Ergonomics

Ergonomics, or design and planning that follows health and safety guidelines, is crucial. The Electricity at Work Regulations 1989 require all electrical systems and equipment to be constructed and maintained in a safe condition. Power cables are carried in trunking that separates them from voice and data cables. Power cables are secured and covered, and do not trail. Suitably qualified staff undertake electrical work. Computer workstations typically have a minimum requirement for two power sockets.

13.3 Working Environment

Levels of lighting in ICT areas are slightly lower than lighting recommendations for standard classrooms, so that there is appropriate contrast between screen and background environment. Where necessary, blackout blinds are installed to reduce the effects of natural daylight. Flooring or carpet in our ICT suites is non-slip and anti-static.

There is a minimum of 1000mm between workstations for one student. There is at least 850mm of clear space in front of the computer table for a chair and circulation space. Where tables are arranged back to back, there is a 1200mm of aisle space between them. This allows wheelchair users to pass. Our arrangement of workstations in the majority of rooms is designed to meet the specific needs of pupils with physical disabilities or other special educational needs.

14. How to Report Misuse or Accidental Access of Inappropriate Materials

Misuse of ICT or accidental access to inappropriate materials is reported to the IT Manager. In both instances, the report should ideally be accompanied by specific details of the materials accessed – for example, a weblink or screen shot. The report must also indicate the date and time on which materials were accessed and a description of the incident.

The report will then be passed on to the Principal and an investigation undertaken, as appropriate to the circumstances. Sanctions for misuse and disciplinary issues are identified below (see 14 Sanctions for misuse).

15. Monitoring by the School

The use of the internet and e-mail raises issues if or when we wish to monitor their use by pupils. As a school we have a right and even a duty to monitor the use of the internet and e-mail systems to prevent it being used inappropriately, for unlawful purposes or to distribute offensive material. However, a student also has a right to fair treatment. It is also the duty of Lincoln Minster School to balance these two separate rights. The first data protection principle states that data should be processed fairly and lawfully. Therefore, we are open on the subject of monitoring and also conduct Computing lessons on the use of the Internet and (internal) e-mail. Pupils currently do not have private school e-mail accounts.

We have the right to take all reasonable steps to prevent pupils from accessing inappropriate material on the internet. However, any monitoring must be proportionate to the risk and designed to prevent rather than detect misuse. In the same way pupils are also taught the importance of keeping personal information private as part of their general awareness of internet and e-mail safety issues. Pupils are also familiar with the concept of data protection, both as a way of protecting information relating to themselves, and in terms of respecting information pertaining to others. As a general rule, children are taught to always question why they are being asked for specific information on web sites or by email, and seek guidance from a teacher or parent/guardian before providing any personal information.

16. Sanctions for Misuse

16.1 Legal implications

Certain behaviours are clearly illegal such as using the internet or e-mail to perpetrate credit card fraud, to spread viruses, to hack into other computers, or to download copyrighted materials. Such issues are covered by the Computer Misuse Act 1990, the Data Protection Act 1998 and copyright legislation.

The school spells out these responsibilities in detail within the AUP.

When developing policies, the school considers possible scenarios of providing student access to internet facilities which might have legal implications, and works through methods of preventing them, or strategies for dealing with them should they arise. For example, the issue of plagiarism, in consultation with the Data Manager, is included within both the ICT AUP and policies covering conduct in internal and external examinations.

16.2 Local enforcement

Local policies are enforced and promoted in equal measure within school and to staff, pupils and parents/guardians alike.

Pupils are made aware of the importance of these policies. Posters outlining the key points and responsibilities are positioned prominently next to all ICT resources. An internet safety education programme based on CEOP materials is delivered at the senior and prep schools.

Local policies are regularly monitored to ensure that they are effective, and reviewed and updated to ensure that they continue to meet the requirements of the school and any emerging uses of technology.

Viruses, spyware and other forms of malware are common now and are usually introduced inadvertently. Lincoln Minster School has an effective, up-to-date software protection against viruses but pupils are also not permitted to undertake any online activity which may increase the risk of exposure to malware. The school has systems for dealing with deliberate misuse of computer systems, including the internet. Depending on the seriousness of the offence, internal sanctions might range from first warnings to temporary bans from using the ICT resources, to involvement of parents and guardians and in extreme cases permanent exclusion (see for example, Appendix 3). Most offences are

likely to be committed by pupils experimenting and testing boundaries. However, if something more serious is suspected – for example, using the internet for illegal purposes, then it may be necessary to involve the police.

Appendix 1: Policy on the Acceptable Use of ICT Facilities by Pupils (Years 7 to 11)

As a pupil at Lincoln Minster School you have good access to computer resources. The computers work across a network and allow you safe, secure and quick access to different electronic resources, printing, the Internet and educational software. Some teachers will also make use of specialised equipment, such as digital video cameras. The network is supported by a team of trained technical staff. The school expects you to use computer resources sensibly and to follow the policy set out below.

You must read and sign this policy before you can be allowed to use Lincoln Minster School computer resources and/or the school network.

Appropriate use of computer resources

- You do not access services that you have not been given permission to use. This includes using computer resources for non-academic work such as party invitations or colour posters.
- You do not print off multiple (more than one) copies of work without permission. Use Print Preview to look at your work and check for any mistakes before sending to the printer.
- You do not access the Internet or e-mail for inappropriate purposes.
- You do not use the Internet or send e-mail if it is not directly related to your school work.
- You do not download, use or upload or send by email any material which is copyright (this means that the material is owned by someone else, for example some music files).

Cyber bullying and e-safety

Cyberbullying is the sending or posting of harmful or cruel text or images using the internet or other digital communication devices, such as mobile phones.

- You do not use mobile phones, including sending or receiving text messages, during the normal school day.
- You do not use strong language, swearing or aggressive behaviour when using the internet or other digital communication devices.
- You do not type anything on a website or send an e-mail that might be offensive.
- You do not force your viewpoint on to others. It is important to be polite at all times.
- You do not give personal information (for example, address or phone number) to anyone on the internet or by e-mail.

Network security and safety

- You do not attempt to bypass network security or filtering.
- As a pupil in KS3 or KS4 (Year 7 to 11) you will not attempt to gain access to the school's WiFi network which is intended for staff and Sixth Form use only.
- You do not give your password or login name to anyone.
- You do not view, upload or download or send by e-mail any material which is likely to be unsuitable for children or schools. This applies to any material of a violent, dangerous, racist,

or inappropriate sexual content. If you are not sure about this, or any materials, you must ask a teacher.

- You agree to the school viewing with just reason and without notice any e-mails you send or receive, material you store on the school's computers, or logs of websites you have visited.

Plagiarism

Plagiarism is the taking of someone else's work, images or ideas and passing this off as your own.

- You do not download information from the internet without identifying where the information came from (for example, Source: www.bbc.co.uk).
- You do not use another's files as if it were your own work, or copy work belonging to someone else and use it as if it were your own.
- You do not use someone else's artwork, pictures or graphics (including graphs, spreadsheets and so on) as if they were made by you.

Failure to comply with any of these rules may result in one or more of the following:

- A ban, temporary or permanent, on the use of the Internet facilities at school.
- A letter informing your parents/guardians of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on access to school facilities to be decided by the Head of Year/Head of Department.
- Temporary or permanent exclusion for abuse of the school's ICT facilities and of the internet.
- Any other action decided by the Principal and Governors of the school.

If you do not understand any part of this Acceptable Use Policy, you must ask a teacher.

LINCOLN MINSTER SCHOOL

Policy on the Acceptable Use of ICT Facilities by Pupils

Declaration by Student

Please sign the statement below to show that you have read and understood the School rules on acceptable use of ICT facilities.

I agree that I have read and understood the school policy on acceptable use of ICT facilities. I understand that if I disobey this policy, the School will take action.

Signed: ..... Date: .....

Name: ..... Form: .....

This sheet is to be returned to your Form Tutor. Thank you.

Policy on the Acceptable Use of ICT Facilities by Pupils (Years 12 & 13)

As a student at Lincoln Minster School you have good access to computer resources and WiFi for your own devices. The computers work across a network and allow you safe, secure and quick access to different electronic resources, printing, the Internet and educational software. Some teachers will also make use of specialised equipment, such as digital video cameras. The network is supported by a team of trained technical staff. The school expects you to use computer resources sensibly and to follow the policy set out below.

You must read and sign this policy before you can be allowed to use Lincoln Minster School computer resources and/or the school network.

Appropriate use of computer resources

- You do not access services that you have not been given permission to use. This includes using computer resources for non-academic work such as party invitations or colour posters.
- You do not print off multiple (more than one) copies of work without permission. Use Print Preview to look at your work and check for any mistakes before sending to the printer.
- You do not access the Internet or e-mail for inappropriate purposes.
- You do not use the Internet or send e-mail if it is not directly related to your school work.
- You do not download, use or upload or send by email any material which is copyright (this means that the material is owned by someone else, for example some music files).

Cyber bullying and e-safety

Cyberbullying is the sending or posting of harmful or cruel text or images using the internet or other digital communication devices, such as mobile phones.

- You do not use strong language, swearing or aggressive behaviour when using the internet or other digital communication devices.
- You do not type anything on a website or send an e-mail that might be offensive.
- You do not force your viewpoint on to others. It is important to be polite at all times.
- You do not give personal information (for example, address or phone number) to anyone on the internet or by e-mail.

Network security and safety

- You do not attempt to bypass network security or filtering.
- You do not give your password or login name to anyone.
- You do not view, upload or download or send by e-mail any material which is likely to be unsuitable for children or schools. This applies to any material of a violent, dangerous, racist,

or inappropriate sexual content. If you are not sure about this, or any materials, you must ask a teacher.

- You agree to the school viewing with just reason and without notice any e-mails you send or receive, material you store on the school's computers, or logs of websites you have visited.

Plagiarism

Plagiarism is the taking of someone else's work, images or ideas and passing this off as your own.

- You do not download information from the internet without identifying where the information came from (for example, Source: www.bbc.co.uk).
- You do not use another's files as if it were your own work, or copy work belonging to someone else and use it as if it were your own.
- You do not use someone else's artwork, pictures or graphics (including graphs, spreadsheets and so on) as if they were made by you.

Failure to comply with any of these rules may result in one or more of the following:

- A ban, temporary or permanent, on the use of the Internet facilities at school.
- A letter informing your parents/guardians of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on access to school facilities to be decided by the Head of Year/Head of Department.
- Temporary or permanent exclusion for abuse of the school's ICT facilities and of the internet.
- Any other action decided by the Principal and Governors of the school.

If you do not understand any part of this Acceptable Use Policy, you must ask a teacher.

LINCOLN MINSTER SCHOOL

Policy on the Acceptable Use of ICT Facilities by Students

Declaration by Student

Please sign the statement below to show that you have read and understood the School rules on acceptable use of ICT facilities.

I agree that I have read and understood the school policy on acceptable use of ICT facilities. I understand that if I disobey this policy, the School will take action.

Signed: ..... Date: .....

Name: ..... Form: .....

This sheet is to be returned to your Form Tutor. Thank you.

Appendix 2: Policy on the Acceptable Use of the Internet by Boarding Pupils

(Pupil copy)

Lincoln Minster School
Internet & e-Safety Rules

Boarding pupils are now granted Internet access in their boarding house, primarily as an essential part of learning, as required by the National Curriculum, but also as a recreational tool. Both pupils and their parents/guardians/carers are asked to sign to show that the Internet and e-Safety Rules have been understood and agreed.

Pupil:	***Boarding House:***

Pupil's Agreement

- I have read and I understand the Boarding House e-Safety Rules.
- I will use the computer, network, Internet access and other new technologies (including mobile phones) in a responsible way at all times.
- I understand that network and Internet access may be monitored.
- I understand that any breach of sensible Internet use will result in withdrawal of such privileges.

Signed:	***Date:***

Parent's/Guardian's Consent for Internet Access
I have read and understood the school e-safety and Internet access rules and give permission for my child to access the Internet in their boarding house. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree to take responsibility for installing appropriate anti-virus software on my child's personal laptop. I agree that the school is not liable for any damages arising from use of the Internet facilities in the boarding house.

Signed:	***Date:***

Please print name:

Please complete, sign and return to your boarding housemaster/mistress

Appendix 3: Exemplar letter detailing action taken when pupil ICT policy infringed

Dear NAME PARENT/GUARDIAN

As you are no doubt aware, we take the issues of computer, and particularly internet, safety very seriously. We have a school wide computer network that is supported by a team of technical staff. Electronic (e-) safety courses are taught within the school curriculum and specific e-safety awareness evenings are offered to parents/guardians. In short, we endeavour to ensure that all members of our school community are aware of both the benefits and the potential dangers of using technology within school.

NAME OF STUDENT has recently attended a compulsory information and awareness lesson on esafety. This is a direct consequence of NAME OF STUDENT by-passing our web filtering software through the use of an external USB drive. The security settings of our network have now been amended to prevent this from occurring in the future.

NAME OF STUDENT is now very aware of our approach on e-safety.

EITHER (if Acceptable Use Policy form returned and signed)

NAME OF STUDENT has signed and returned the policy on e-safety.

OR

However, NAME OF STUDENT has not yet signed and returned the school policy on **Acceptable Use of ICT Facilities**. Unfortunately, if we do not receive a signed copy of the agreement, then we will need to remove all their access to ICT within school. A copy of the Acceptable Use Policy is included.

Please take the opportunity to speak with NAME OF STUDENT regarding issues of e-safety. Should we find evidence that there has been unacceptable use of technologies in school in the future, then further action will be taken.

Kind regards

Deputy Head, Teaching and Learning