

Lincoln Minster School

Acceptable Usage of ICT – Staff

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 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
- Mobile phone policy
- Social media policy
- Bring your own device and personal device policy document

This policy applies to all staff in our school community, including those in the boarding community and EYFS.

Lincoln Minster School is committed to ensuring that the application of this policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunities policy document.

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 documents: Academic Integrity, Acceptable use of ICT for Pupils, Anti-Bullying, Behaviour, Child Protection, Controlled Assessment, Curriculum, Equal Opportunities, Health and Safety, Mobile Phone, Social Media and United Learning Staff-Student Relationships Guidance.

This document is reviewed annually by the IT Manager or as events or legislation change requires. The next scheduled date for review is September 2026

Reviewed By	George Kellow; IT Manager
Approved By	Jon Tyler – Headteacher
Date	September 2025
Reason for Change	Annual Review
Next review date	September 2026

Contents

1.	<i>Policy Statement</i>	<i>Page 1</i>
2.	<i>Key Personnel</i>	<i>Page 4</i>
3.	<i>Introduction</i>	<i>Page 4</i>
4.	<i>Educational ICT Vision</i>	<i>Page 4</i>
5.	<i>Use of Email and the Internet</i>	<i>Page 5</i>
6.	<i>Use of Social Media, Instant Messaging and Chat Rooms</i>	<i>Page 6</i>
	<i>6.1 Implementation</i>	<i>Page 7</i>
7.	<i>Copyright</i>	<i>Page 7</i>
8.	<i>Private Usage Policy</i>	<i>Page 8 - 11</i>
8.1	<i>Legislation</i>	<i>Page 8</i>
8.2	<i>Personal Use of School Provided Devices</i>	<i>Page 8</i>
8.3	<i>Use of Personal Devices on the School Network</i>	<i>Page 9</i>
8.4	<i>Use of Personal Storage Devices</i>	<i>Page 9</i>
8.5	<i>Data Security</i>	<i>Page 10</i>
8.6	<i>Data Protection</i>	<i>Page 10</i>
8.7	<i>Freedom of Information</i>	<i>Page 11</i>
8.8	<i>Passwords</i>	<i>Page 11</i>
8.9	<i>Permission</i>	<i>Page 11</i>
9.	<i>Health and Safety</i>	<i>Page 11</i>
9.1	<i>Regulations</i>	<i>Page 12</i>
9.2	<i>Ergonomics</i>	<i>Page 12</i>
9.3	<i>Working Environment</i>	<i>Page 12</i>
10.	<i>How to Report Misuse or Accidental Access to Inappropriate Images</i>	<i>Page 13</i>
11.	<i>Monitoring by the School</i>	<i>Page 13</i>
12.	<i>Sanctions for Misuse</i>	<i>Page 13</i>
12.1	<i>Disciplinary Issues</i>	<i>Page 14</i>
13.	<i>Training and CPD</i>	<i>Page 14</i>
13.1	<i>School Leaders</i>	<i>Page 14</i>
13.2	<i>Teaching and Support Staff</i>	<i>Page 14</i>
13.3	<i>Technical Staff</i>	<i>Page 15</i>
	<i>Appendix 1: Staff Acceptable Usage of ICT Policy Agreement</i>	<i>Page 16</i>
	<i>Appendix 2: Display Screen Equipment – Workplace Safety for Staff, Pupils and Visitors</i>	<i>Page 18</i>

2. Key personnel

Senior School	Nicholas Boot	Deputy Head – Head of Digital Strategy
Prep School	Rebecca Dickson	Head of E-Learning
Boarding	Charlotte Brigden	Assistant Head (Pastoral)

3. 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. 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 students' 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 because 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 be 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.

4. 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 include 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. Interactive whiteboard training is offered and this training, along with ICT resourcing, combines with exciting and innovative teaching practices to help ensure that students 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.

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 students and to facilitate best teaching practice by teachers. Administrative systems must be used to improve effectiveness, achieve efficiencies and promote best practice. Line managers have responsibility to ensure that ICT usage achieves all of the above.

5. Use of Email and the Internet

Internet and e-mail access is to be used for business purposes. However, limited and responsible personal use of the internet is permissible provided it takes place during breaks or personal time. Staff must understand that privacy is not guaranteed and restrictions to non-business internet sites may be applied. Any personal data created or accessed through e-mail, the internet or through any computer programme may be viewed or accessed by the IT Manager without the employee's permission.

Communication systems must not be used for conveying messages that may be considered defamatory, derogatory, obscene, discriminatory or are otherwise abusive or inappropriate. Harassment is a serious offence that will be dealt with through the Disciplinary Procedure and Anti-Harassment and Bullying ('Dignity at Work') Procedure. Any inappropriate material inadvertently received by e-mail which may cause offence to others must be deleted immediately and its receipt reported to the member of staff's Line Manager. The definition of 'inappropriate material' for the purposes of this policy is anything which could potentially be illegal or potentially offensive to others.

Staff must not issue the school web address to any site that is filtered by the school and therefore is intentionally inaccessible from the school network (e.g. some social networking sites). Staff must also not issue their work e-mail addresses to any companies that may generate excessive junk mail.

Examples include:

- Sexually explicit material or offensive language;

- Racist, politically offensive, sexist, hate material or offensive language.

Under no circumstances must material received from an internal or external source that is not strictly for business purposes be passed on to any other system user or to any other e-mail address. It must not be stored on any network drive, local drive or removable media such as memory sticks or other removable media.

Defamation is the publication of a statement that adversely affects a person's or an organisation's reputation, for which legal action may be taken against the sender. Staff must not send or circulate negative information about an individual or organisation without first checking that the contents are accurate and obtaining permission from their Line Manager. Defamation of the school would be seen as a breach of an employee's contract of employment.

Use of electronic information carries with it a risk of breach of confidence. Staff must be aware of their obligations under the school guidance with respect to personal and sensitive data, and commercially or otherwise confidential information. Such information must not be transmitted by e-mail or the internet.

Viewing, circulating, or downloading pornographic material is a serious abuse of this policy and will be dealt with under the Disciplinary Procedure as gross misconduct. Viewing of illegal material will be dealt with by reporting it to the police. Staff must ensure that copyright laws are not infringed by the downloading or circulation of material from the internet.

Staff must read and sign an Acceptable Usage Policy agreement before they can be allowed to use the Internet or e-mail at school (Appendix 1). This forms part of the contractual agreement of employment and is signed prior to the start date of employment. The Headmaster's P.A. keeps a copy of the signed agreement, which is filed with the accompanying contract of employment and pre-employment checks. Staff also sign an updated copy of this document at the beginning of each academic year.

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

This is supported by the Social Media Policy.

So-called Web 2.0 social software such as Facebook and Twitter provide 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.

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. Unfortunately, these sites can also be the ideal platform for facilitating bullying, slander and humiliation of others

The majority of social networking sites are not allowed in school and are blocked by the web filtering software. Staff are given clear guidelines in the United Learning Staff-Students Relationships Guidance document, issued annually, prohibiting them from contacting or communicating with current pupils or those who have recently left via social networking sites.

6.1 Implementation

Clearly banning activity of any sort merely heightens the desire of young people to explore and push the boundaries. We have a responsibility to understand what children are doing by talking to them about their online activity and educating them to the possible downsides - encouraging safe use and enjoying the benefits whilst minimising the risks. Consequently, at Lincoln Minster School we

- Use and refer to a separate Social Media policy
- 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 the IT Manager and/or by the Senior Leadership Team
- Provide timely and accurate information for parents and teachers e.g. CEOP awareness evenings to parents
- Provide safety tips and good advice
- Stay up to date on developments e.g. via the United Learning ICT Newsletter

7. Copyright

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 Copyright Licensing Agency (CLA) 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.

8. Private Usage Policy

Computing facilities are provided for the school's business purposes and responsible personal use may be allowed at the Headmaster's discretion provided there is no conflict with the interests or requirements of the school. The school does not accept liability for any personal loss or damage incurred through using the school computing facilities for private use.

8.1 Legislation

The following are a list of Acts that apply to the use of the school computing facilities and which must be adhered to:

- Regulation of Investigatory Powers Act 2000;
- Computer Misuse Act 1990;
- Protection from Harassment Act 1997;
- Sex Discrimination Act 1975;
- Race Relations Act 1976;
- Disability Discrimination Act 1995;
- Obscene Publications Act 1959;
- Telecommunications Act 1984;
- Protection of Children Act 1978;
- Criminal Justice Act 1988;
- Data Protection Act 1998;
- The Patents Act 1977;
- Copyright, Designs and Patents Act 1988;
- Defamation Act 1996;
- Freedom of Information Act 2000;
- Human Rights Act 1998.

We promote the highest standards in relation to good practice and security in the use of information technology. Consequently we expect and support the integrity of our employees. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

8.2 Personal Use of School Provided Devices

Lincoln Minster School will provide staff with a tablet device for use in the classroom. While a staff member is employed at Lincoln Minster School they will have responsibility for this device and may choose to take it home to use for school purposes or for personal purposes. If a staff member chooses to use their devices for personal purposes, or to store personal data on the device they should do so in accordance with the following stipulations. These stipulations are in place in order to protect the safeguarding of both staff and pupils:-

- You must protect the device via a complex password (8 characters or greater, including numbers, letters, upper and lower case) or a biometric measure.
- You must set up the device to auto-lock after a set period of idleness.

- In the event that your device is lost, stolen or destroyed, you must inform the ICT Helpdesk and immediately change all passwords related to your access to United Learning systems.
- You must keep any personal data separate from United Learning data. The simplest way to achieve this is to use the OneDrive client which the ICT Helpdesk will set up for you.
- Data must at all times remain within United Learning systems – emails should not be forwarded to private accounts and files should only be stored within OneDrive rather than saved locally.
- Transferring data out of United Learning systems for use elsewhere using non-approved cloud storage services (Dropbox, Google Drive, etc.) is not permitted. Doing so heightens the risk that data will leave United Learning's control.
- Do not engage in risky activities using the tablet device in your private life. For example, visiting websites with gambling, adult or illegal content would place the device at greater risk of malware infection and hijacking.
- You must not allow any non-employee of United Learning to access your device, including family members.
- You must not modify the Operating System in order to 'jailbreak' your device (this means attempting to remove restrictions which the manufacturer has built into their system). This weakens a device's security as usually software patches will not be installable from that point on.

8.3 Use of Personal Devices on the School Network

Lincoln Minster School does not support nor allow any use of personal devices on the wired school network (Laptops, netbooks, tablets and mobile phones). Personal devices may be used in school but will not work across the wired school network. There is no technical support provided for personal devices and requests for technical support, including the configuration of personal devices to work across the wired school network, will be declined.

Any member of staff using a personal device at school should familiarise themselves with the *Bring Your Own Device* policy document to ensure procedures are followed correctly.

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

8.4 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.

8.5 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. It is policy to store data on a network drive where it is regularly backed up. Schools must ensure that data that is not stored on the network file server is regularly backed up. Any mobile storage devices such as USB pen drives or external hard disks that include pupil data or any other data covered by the 1998 Data Protection Act, should be appropriately encrypted, although great care should be taken with using the devices to ensure that personal, confidential information or sensitive corporate data is not taken off-site. Care should also be taken if the data network is used for the transmission or storage of CCTV images to ensure that legal requirements are met.

Any member of staff using a personal storage device should familiarise themselves with the *Bring Your Own Device* policy document and the procedure for secure transfer of files policy document to ensure procedures are followed correctly.

8.6 Data Protection

United Learning maintains a notification to the Data Protection Commission in compliance with the Data Protection Act 1998. This notification is held on a public register and contains details of the organisation's holding and processing of personal data. The Data Protection Compliance officer must be informed of all collections of personal data through the annual audit. It is the responsibility of all school staff to ensure that personal data is held and processed within the terms of United Learning notification and in compliance with the data protection principles. Personal data shall be:

- obtained and processed fairly and lawfully;
- held for specified lawful purpose(s);
- not used or disclosed in a way incompatible with the purpose(s);
- adequate, relevant and not excessive for the purpose(s);
- accurate and up to date;
- not kept longer than necessary;
- available to the data subject;
- kept secure.

Staff should note that all data and correspondence, including e-mail messages, held by the school may be provided to a data subject, internal or external, in the event of a subject access request.

8.7 Freedom of Information

Schools are subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. Employees should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Therefore, such data or correspondence may be provided to an applicant in the event of an access request once the Act has come into force.

8.8 Passwords

Passwords protect school systems from access by unauthorised people. Therefore network passwords should never be given to anyone else without departmental manager's permission. 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 school should not allow the connection of non-corporate computer equipment to the network without prior written request and technical approval. This includes connection via dialup or Virtual Private Networking (VPN).

8.9 Permission

Users must obtain prior approval at a senior management level to:

- set-up internet sites on school computing facilities;
- publish pages on external internet sites containing information relating to the school;
- enter into agreements on behalf of themselves or the school via a network or electronic system;
- transmit unsolicited commercial or advertising material to other users of a network or to other organisations;
- use school computing facilities for external business interests or personal gain.

9. Health and Safety

Most ICT-related health and safety issues are dealt with 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".

9.1 Regulations

The use of display screen equipment by students, teachers and non-teaching staff is covered by this policy and all workstations at which school members work should comply with the minimum requirements;

- an assessment is carried out by the user of each workstation and this is recorded. The assessment is carried out annually and includes a review of the workstation itself (display screen plus furniture), the environment and the interface between the computer and user. This assessment is carried out by the individual user using the VDU workstation checklist in Appendix 2. The checklist is provided as an e-mail attachment and is sent out by the school Health and Safety Officer. The completed checklist is returned to the Health and Safety Officer.
- once an assessment has been carried out, the Health and Safety Officer directs the Technical Department to undertake any remedial action, as indicated by the checklist.
- 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;
- where any employee user requests one, the school must arrange and pay for an eye and eyesight test by a registered ophthalmic optician and this should be repeated at a frequency recommended by the optician;
- where separate spectacles are recommended for use with display screens, the cost of a basic pair of glasses must also be met by the employer;
- all users are provided with health and safety training about their equipment but in practical terms there is likely to be considerable overlap between the training on the uses of the equipment, the software etc. and the health and safety training (information on possible ill health effects e.g. upper limb pain, eyesight defects, fatigue and stress etc. should also be given);
- there are no ionising radiation problems associated with display screens.

9.2 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 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. All computer workstations have a minimum of two power sockets.

9.3 Working Environment

Levels of lighting in Computing areas is 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 Computing 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.

10. 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 web link or screen shot. The report must also indicate the date and time when materials were accessed and a description of the incident.

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

11. Monitoring by the School

Lincoln Minster School may monitor without notice external and internal e-mail and internet usage including length of use, sites visited and has the right if it wishes to have access to read any matter sent or received by its staff. Lincoln Minster School may monitor and assess files to ensure compliance with policy and for the reasons set out above and, in particular, to prevent the use of computer facilities for discriminatory purposes or harassment, an/or the commission of a criminal offence. This is communicated in writing to all employees via this policy and the Staff Handbook.

12. Sanctions for Misuse

Penalties for misuse of computer systems will depend on the nature and seriousness of the offence. Disciplinary action may be taken against employees who contravene this policy. The school, for various legitimate business practices, may need to monitor the use of e-mail and internet access from time to time for the following reasons:

- to establish the existence of facts (e.g. the details of an agreement made);
- to monitor for quality control and staff training purposes;
- to prevent or detect crime;
- to investigate or detect unauthorised use of the school's telecommunication system (including e-mail and internet);
- to intercept for operational purpose such as protecting against viruses and making routine interruptions such as forwarding e-mail to correct distributions; and
- to gain access to routine business communications (e.g. checking e-mail) when staff are on holiday or sick leave.

Should an employee have their access to the internet and e-mail withdrawn, with or without notice, and wish to appeal against this decision, this should be done via the United Learning Grievance procedure.

12.1 Disciplinary Issues

Examples of behaviours which may require the use of the Disciplinary policy include:

- criminal acts, for example in relation to child abuse images;
- visiting pornographic sites ;
- harassment in the form of inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace;
- obscene, racist jokes or remarks which have been shared internally and externally and which may reflect on the image of employer and bring the organisation into disrepute;
- downloading and installation of unlicensed products;
- viewing non-pornographic but sexually explicit materials, except where this forms an authorised part of the employee's job (for example to support the teaching of A-level biology);
- chat rooms, especially for sexual discourse or to make arrangements for sexual activity;
- violation of the school's other legal obligations such as software media counterfeiting or illegitimate distribution of copied software.

The school has the right to monitor employees' or students' use of computer equipment where there is evidence to suggest misuse. (Regulation of Investigatory Powers Act 2000).

13. Training and CPD

13.1 School Leaders

At Lincoln Minster School, leaders and governors understand the potential of technology and are able to harness it, so that it is used effectively to produce the best possible learning experiences for students.

At Lincoln Minster School, the Deputy Head (Academic) works alongside other members of the Senior Leadership Team in order to ensure a programme of training and support for all staff that is appropriate. An annual update and refresher training is delivered within the CPD programme at the start of the academic year.

13.2 Teachers and Support Staff

ICT and e-Learning Training and CPD for teachers and support staff is planned to ensure that:

- They are directly relevant to learning and teaching
- Intended outcomes are clearly defined
- Previous knowledge and expertise are taken into account
- They model effective teaching and learning strategies
- Impact evaluation is planned from the outset

13.3 Technical Staff

The technical staff play a vital role at Lincoln Minster School. They provide technical and network support, including troubleshooting and resolving ICT user problems and undertaking specific maintenance and upgrade tasks for school networks.

The best practice for technical support is implemented within the group through the Framework for IT Support (FITS) and Technical Competencies Framework which identifies how staff can progress their careers.

The Bursar line manages the IT Manager. This helps to ensure that there is a robust and an appropriate technical framework to support the needs of safe teaching and learning.

Appendix 1: Staff Acceptable Usage of ICT Policy Agreement

ICT Acceptable Use Policy; Academic Year 2025 – 26

All employees must read and sign this Acceptable Use Policy on appointment before they can be allowed to use devices or services provided by or on behalf of United Learning, and then on an annual basis. In signing this policy, you agree to the following:

- a. An authorised representative of the Group may view, with just reason and without notice or notification, any communications you send or receive, material you store on the Group's computers/ services or logs of websites you have visited. This data, regardless of where hosted, belongs to United Learning at all times. It is the Group's policy not to view colleagues' emails without good cause.
- b. You will only access those services/ aspects of services which you have been given permission to use.
- c. You will not use United Learning resources to operate your own business.
- d. You will not attempt to remove any of the security measures put in place by United Learning to ensure the integrity of its services, the security of its data or the appropriateness of employee activity.
- e. Any communication from a United Learning related account (email, social media) or account which identifies you as belonging to United Learning will be appropriate in tone and content.
- f. You will exercise caution when sending information via email to ensure that it is addressed to the correct recipient(s) and is the correct information (particularly when attaching documents). Personal data (that by which an individual could be identified) must not be transferred to other recipients unless encrypted or password protected, in line with the requirements of Data Protection legislation.
- g. You will not transfer United Learning data outside of the organisation's systems except via Group email or encrypted media. This includes the use of cloud storage and personal email accounts. *For example, saving files to Dropbox or emailing them to a personal Hotmail account may resolve logistical problems you are having but run the risk of those data leaving United Learning's control.*

- h. You will use the Internet and other services for appropriate activity only. United Learning considers inappropriate activities to include gambling (outside of workplace Lottery syndicates), pornography and sites promoting views which run counter to the organisation's ethos.
- i. You will not share your access credentials with anyone. Delegated access to calendars/ email should be granted to administrative support staff, where required.
- j. You will not download, use, distribute or otherwise communicate any material which, in so doing, infringes copyright.
- k. The use of language deemed aggressive, offensive or intimidating is not acceptable. You must not write anything on a website or send by email or other medium anything which could be reasonably be deemed offensive.
- l. Use of a personal device to access any United Learning data is permitted, subject to the acceptance of the separate Bring Your Own Device policy.
- m. Breach of this policy may result in disciplinary action.

Name:	
Signature:	
Job Title:	
Date:	

Please return your completed form to Vicki Bowkett.

Appendix 2: Display Screen Equipment – Workplace Safety for Staff, Pupils and Visitors

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”.

The use of display screen equipment (DSE) by pupils is not covered by the Regulations but all workstations at which employees work should comply with the minimum requirements.

Likely “users” are secretaries, word-processing workers, accountants and accounts staff. The definition of a user depends on the nature and the extent of use and applies to full and part-time staff. Typically, continuous or near continuous spells of DSE work for an hour or more at a time most working days classifies an employee as a user. It is likely that there will only be a small number of users.

An assessment must be carried out on the workstations of each user on initial identification of need and this should be recorded; the assessment must be carried out using the VDU workstation checklist following; and once an assessment has been carried out, any remedial action, as indicated by the checklist must be taken. Assessments must be regularly reviewed.

Where any employee “user” requests one, the employer must arrange and pay for an eyesight test by a registered ophthalmic optician and this should be repeated at a frequency recommended by the optician.

Where separate spectacles are recommended for use with DSE, the cost of a basic pair of glasses must also be met by the employer.

All users must be provided with health and safety training about their equipment but in practical terms, there is likely to be considerable overlap between the training on the uses of the equipment, the software etc. and the health and safety training. (Information on possible ill health effects such as upper limb pain, eyesight defects, fatigue and stress etc. should also be given).

There is no ionising radiation problem associated with display screens.

(Sample of checklist follows)

Requirement – assessments must be undertaken using the form following which can also be used for self assessment. Line managers must check the assessments. It is their duty to follow through any actions identified.

VDU Workstation Risk Assessment Form

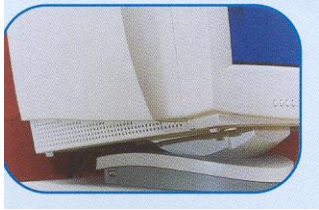
Workstation location	
User:	

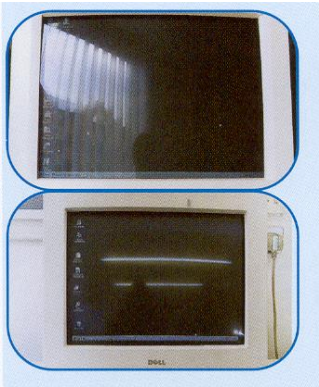
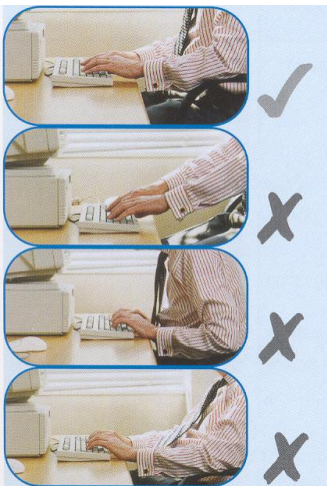
Checklist completed by:	
Assessment checked by:	
Date of assessment:	
Any further action needed?	YES / NO
Follow-up action completed on:	

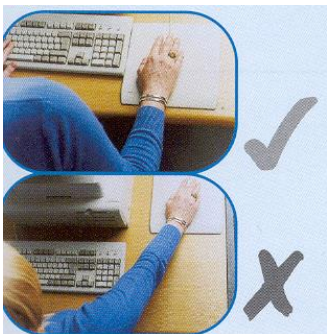
This checklist can be used as an aid to risk assessment and to help comply with the Schedule to the Health and Safety (Display Screen Equipment) Regulations.

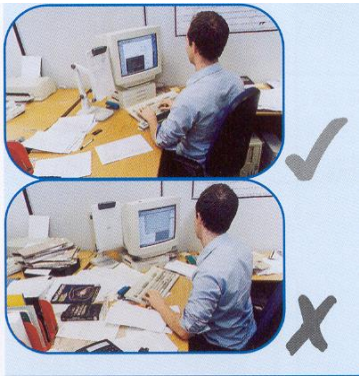
Work through the checklist, with the employee sitting at their usual workstation, ticking either the 'yes' or 'no' column electronically against each risk factor:

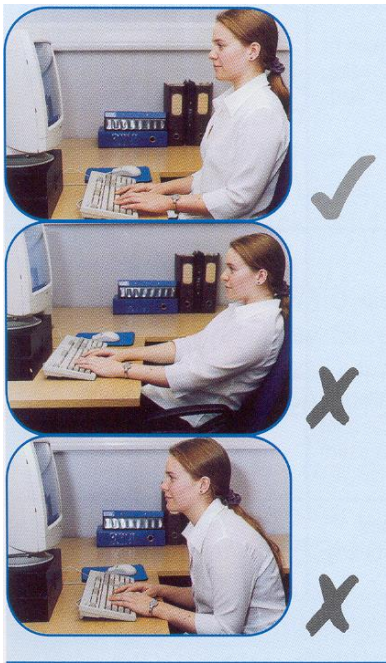
- 'Yes' answers require no further action
- 'No' answers will require investigation and/or remedial action by the workstation assessor who should record their decisions in the 'Action to take' column. The relevant manager should check later that actions have been taken and have resolved the problem.

Risk factor	Tick answer		Things to consider	Action to take
	Yes	No		
1 Display screens				
Are the characters clear and readable? 			Make sure the screen is clean and cleaning materials are made available. Check that text and background colours work well together.	
Is the text size comfortable to read?			Software settings may need adjusting to change text size.	
Is the image stable, i.e. free of flicker and jitter?			Try using different screen colours to reduce flicker, eg darker background and lighter text. If problems still exist, get the set-up checked, eg by the equipment supplier.	
Is the screen's specification suitable for its intended use?			For example, intensive graphic work or work requiring fine attention to small details may require large display screens.	
Are the brightness and/or contrast adjustable?			Separate adjustment controls are not essential, provided the user can read the screen easily at all times.	
Does the screen swivel and tilt? 			Swivel and tilt need not be built in; you can add a swivel and tilt mechanism. However, you may need to replace the screen if: • swivel/tilt is absent or unsatisfactory; • work is intensive; and/or • the user has problems getting the screen to a comfortable position.	

Risk factor	Tick answer		Things to consider	Action to take
	Yes	No		
Is the screen free from glare and reflections? 			Use a mirror placed in front of the screen to check where reflections are coming from. You might need to move the screen or even the desk and/or shield the screen from the source of reflections. Screens that use dark characters on a light background are less prone to glare and reflections.	
Are adjustable window coverings provided and in adequate condition?			Check that blinds work. Blinds with vertical slats can be more suitable than horizontal ones. If these measures do not work, consider anti-glare screen filters as a last resort and seek specialist help.	
2 Keyboards				
Is the keyboard separate from the screen?			This is a requirement, unless the task makes it impracticable (eg where there is a need to use a portable).	
Does the keyboard tilt?			Tilt need not be built in.	
Is it possible to find a comfortable keying position? 			Try pushing the display screen further back to create more room for the keyboard, hands and wrists. Users of thick, raised keyboards may need a wrist rest.	
Does the user have good keyboard technique?			Training can be used to prevent: - hands bent up at wrist; - hitting the keys too hard; - overstretching the fingers.	

Risk factor	Tick answer		Things to consider	Action to take
	Yes	No		
Are the characters on the keys easily readable?			Keyboards should be kept clean. If characters still can't be read, the keyboard may need modifying or replacing. Use a keyboard with a matt finish to reduce glare and/or reflection.	
3 Mouse, trackball etc				
Is the device suitable for the tasks it is used for?			If the user is having problems, try a different device. The mouse and trackball are general purpose devices suitable for many tasks, and available in a variety of shapes and sizes. Alternative devices such as touch screens may be better for some tasks (but can be worse for others).	
Is the device positioned close to the user? 			Most devices are best placed as close as possible, eg right beside the keyboard. Training may be needed to: • prevent overreaching; • tell users not to leave their hand on the device when it is not being used; • encourage a relaxed arm and straight waist	
Is there support for the device user's wrist and forearm?			Support can be gained from, for example, the desk surface or arm of a chair. If not, a separate supporting device may help. The user should be able to find a comfortable working position with the device.	
Does the device work smoothly at a speed that suits the user?			See if cleaning is required (eg of mouse ball and rollers). Check the work surface is suitable. A mouse mat may be needed.	
Can the user easily adjust software settings for speed and accuracy of pointer?			Users may need training in how to adjust device settings.	
4 Software				

Risk factor	Tick answer		Things to consider	Action to take
	Yes	No		
Is the software suitable for the task?			Software should help the user carry out the task, minimise stress and be user-friendly. Check users have had appropriate training in using the software. Software should respond quickly and clearly to user input, with adequate feedback, such as clear help messages.	
5 Furniture				
Is the work surface large enough for all the necessary equipment, papers etc? 			Create more room by moving printers, reference materials etc elsewhere. If necessary, consider providing new power and telecoms sockets, so equipment can be moved. There should be some scope for flexible rearrangement.	
Can the user comfortably reach all the equipment and papers you need to use?			Rearrange equipment, papers etc to bring frequently used things within easy reach. A document holder may be needed, positioned to minimise uncomfortable head and eye movements.	
Are surfaces free from glare and reflection?			Consider mats or blotters to reduce reflections and glare.	
Is the chair suitable? Is the chair stable? Does the chair have a working: • seat back height and tilt adjustment? • seat height adjustment? • swivel mechanism? • castors or gliders?			The chair may need repairing or replacing if the user is uncomfortable, or cannot use the adjustment mechanisms.	

Risk factor	Tick answer		Things to consider	Action to take
	Yes	No		
Is the chair adjusted correctly? 			The user should be able to carry out their work sitting comfortably. Consider training the user in how to adopt suitable postures while working. The arms of chairs can stop the user getting close enough to use the equipment comfortably. Move any obstructions from under the desk.	
Is the small of the back supported by the chair's backrest?			The user should have a straight back, supported by the chair, with relaxed shoulders.	
Are forearms horizontal and eyes at roughly the same height as the top of the VDU?			Adjust the chair height to get the user's arms in the right position, and then adjust the VDU height, if necessary.	
Are feet flat on the floor, without too much pressure from the seat on the backs of the legs?			If not, a foot rest may be needed.	
6 Environment				
Is there enough room to change position and vary movement?			Space is needed to move, stretch and fidget. Consider reorganising the office layout and check for obstructions. Cables should be tidy and not a trip or snag hazard.	

Risk factor	Tick answer		Things to consider	Action to take
	Yes	No		
Is the lighting suitable, eg not too bright or too dim to work comfortably? 			Users should be able to control light levels, eg by adjusting window blinds or light switches. Consider shading or repositioning light sources or providing local lighting, eg desk lamps (but make sure lights don't cause glare by reflecting off walls or other surfaces).	
Does the air feel comfortable?			VDUs and other equipment may dry the air. Circulate fresh air if possible. Plants may help. Consider a humidifier if discomfort is severe.	
Are levels of heat comfortable?			Can heating be better controlled? More ventilation or air-conditioning may be required if there is a lot of electronic equipment in the room. Or, can users be moved away from the heat source?	
Are levels of noise comfortable?			Consider moving sources of noise, eg printers, away from the user. If not, consider soundproofing.	
7 Final questions to users ...				
Ask if the checklist has covered all the problems you may have working with their VDU. Ask if you have experienced any discomfort or other symptoms which you attribute to working with their VDU. Ask if the user has been advised of their entitlement to eye and eyesight testing. Ask if the user takes regular breaks working away from VDUs.				

Write the details of any problems here: