Online Safety Awareness and Education

This policy is complementary to other College policies, particularly those relating to Child Protection & Safeguarding, Promotion of British Values and Managing Student Behaviour through Recognition, Rewards and Positive Action.

This policy has taken account of the following documentation:

i) 'The Byron Review' – Dr Tanya Byron, 2008

ii) 'The safe use of new technologies' – OFSTED, February 2010

iii) 'Data Protection Act' – HM Government, 1998

iv) The Prevent Duty – HM Government, 2015

v) Keeping Children Safe in Education – HM Government, 2016

Context

Landau Forte College Derby is committed to the use of the Internet and other expanding technologies within education. Whilst the growth of digital information technologies is positive and provides many learning opportunities, it also carries with it potential risks if misused. As in any other area of their lives, students are vulnerable to inappropriate material and danger. Furthermore, the College recognises the use of the Internet to promote Terrorist and Extremist material and alongside other illegal material will ensure that students are guarded against this. By being better informed of the issues and potential risks, students will be more able to recognise when they might be in danger and to take proactive measures to safeguard themselves. Similarly, advances in technology offer new challenges for staff and it is equally important that they are mindful of both the risks and challenges, as well as the benefits to facilitating effective learning.

Under our duty of care, Landau Forte College Derby has the responsibility to use new technologies in order to equip students with the skills to access life-long learning and to further themselves in employment. To achieve this, the College has a commitment to provide superior ICT equipment and internet access, as well as clear guidance on its safe use, as part of the students' learning experience.

This policy addresses the issues surrounding the safe and secure use of the College's ICT system. Students are not required to bring any personal electronic

device into College, and do so at their own risk. Students' own devices are not connected to the College's wireless network (see also 1f and 7c).

Purpose

To ensure that all students and staff are aware of the opportunities and dangers provided by the ever expanding area of ICT and are best placed to protect themselves and use the equipment appropriately and safely.

Objectives and Procedures

1. Educate students in the correct use of electronic systems:
    a. There will be an age specific curriculum educating students in all aspects of safe online behaviour. Curricular provision will be reviewed regularly by the Online Safety committee. At KS3, this will take place predominantly in Computing sessions. At KS4 and KS5, this provision will be mainly covered in Life Learning sessions.
    b. In addition to an age specific curriculum, the College will raise the profile of online safety through themed days, events and gatherings. These include Safer Internet Day and RISK week and involve a range of activities during Personal Tutorial Time
    c. Students will be advised never to give out personal details of any kind which may identify them or their location.
    d. Students will be taught to be critically aware of the materials they read using internet sources and shown how to validate information before accepting its accuracy.
    e. Students will be made aware of how to report abuse/inappropriate material both within and outside of College.
    f. During the standard college day, students will be expected to use personal electronic devices including mobile phones for College business purposes only. Examples of this include the use of the College App, calendars to aid organisation and other approved applications such as Show My Homework.
    g. Any misuse of mobile phones, or any personal electronic devices, will be addressed in accordance with the College's complementary policy, Managing Student Behaviour through Rewards, Recognition and Positive Action and may result in the confiscation of the device Misuse of mobile technologies includes but is not limited to taking photographs or videos of other students/staff and playing games or game applications

2. Train staff in the appropriate and corporate use of electronic systems:
    a. E-mails will be used for college purposes only and use will be in accordance with the staff AUP (Appendix 1) and terms and conditions of employment.
    b. Staff will use a corporate signature for all e-mails sent to external agencies (Appendix 2)
    c. When sending e-mails to external agencies, staff will, where appropriate and in accordance with the Data Protection Act 1998, secure personal information and/or use secure e-mail access.
    d. In line with other communication, when e-mailing parents/carers staff will not disclose personal details of other students.
    e. The College will ensure that staff remain up-to-date with the understanding of online safety issues through regular staff updates and training. This includes the Prevent Duty. Staff delivering on the age-appropriate curriculum will receive CEOP approved training cascaded from CEOP ambassadors amongst the staff.

3. Inform and empower parents/carers to be fully aware of their child's use of electronic systems:
    a. The College will raise awareness amongst parents/carers through incorporating online safety awareness into formal evenings and events over the course of an academic year.
    b. Online Safety awareness will form part of the agenda for student consultations.
    c. The College's website will provide links to where parents and students can get further support and guidance.

4. Manage web filtering, e-mail and portable storage:
    a. The College will provide a web filter that will screen all student and staff usage of the internet. The filter will be set at a different level of sensitivity for students in KS3, KS4, KS5 and for staff. This will be reviewed at least on a yearly basis by the online safety committee to ensure that the web filtering methods selected are appropriate, effective and reasonable and ensure that students are safe from accessing illegal, terrorist or extremist material
    b. In addition to providing a web filter, all use of the internet will be recorded and monitored by the Systems Management Team to ensure the continued safety and security of its users. Where inappropriate use of the internet is discovered, action will be taken in line with procedures in Section 8 of this policy.
    c. The College will operate a virus checker on all e-mails and portable devices used on the system. The Systems Management Team will ensure that all measures to protect students/staff are reviewed and improved regularly.

d. E-mails sent within the College and across the Trust will be secure. External e-mails will contain a trust-wide disclaimer (Appendix 4)
e. In the event that staff or students discover an unsuitable site, it will be reported to the Online Safety Coordinator, or the Systems Management Team.

5. Manage existing and emerging technologies:
    a. Guidance will be provided for staff on the use and security of college laptops both in and out of College as part of the contract signed when college laptops are issued.
    b. New and emerging technologies will be researched by the Systems Management Team where they will be examined for education benefit. A risk assessment will be carried out before use in College is allowed.
    c. The College will have an Online Safety committee comprising the Online Safety coordinator (Vice Principal), Director of Learning for Mathematics, ICT and E-Learning, Systems Support Technician, and Child Protection & Student Support Manager. The committee will meet regularly (bi-termly) to review online safety provision across the College.

6. Protect personal/sensitive data – including adherence to the Data Protection Act (1998):
    a. The College operates a Secure Password Policy (Appendix 5) to emphasise that student and staff user areas and files are kept secure and Landau Forte College identities remain private.
    b. Only authorised personnel will be able to edit data held on the systems and appropriate restrictions will be placed on certain folders to limit access to appropriate staff only, for example, folders containing child protection logs.
    c. It is the responsibility of staff to ensure the security of any personal, sensitive, confidential or classified information contained in documents or software such as SIMS (Appendix 6)
    d. It is similarly the responsibility of staff to ensure the security of sensitive information that is either: faxed, copied, scanned, printed, FTP'd, emailed or held on an electronic device, such as a portable hard drive or memory stick. This is particularly important when shared printers/copiers or public areas are used.

7. Manage social networking and personal publishing:
    a. Landau Forte College will block student access to any social networking sites.
    b. Although unable to access social networking sites on the College's system, opportunities will be provided within the curriculum for students to discuss safe social networking in context in accordance with Objective 1. They will be advised on social network security, encouraged to deny access to unknown individuals and shown how to

block unwanted communications for when they use social networking sites outside of College whether on mobile, tablet or PC device. Self-help guides for major social networking sites are available for downloading from the College website

c. Instances where students have posted or sent inappropriate, offensive, abusive or explicit messages/photos will be dealt with according to Section 8 of this policy and with adherence to the policies on Managing Behaviour through Rewards, Recognition and Positive Behaviour and Child Protection & Safeguarding. In accordance with legal requirements, all sexually explicit images discovered will be reported to the Police by the Child Protection Manager.

8. Manage the use of systems through a robust Acceptable Use Policy (AUP):
    a. The College will ensure that the AUP (Appendix 4) is signed by every student and parent/carer of students at the college.
    b. Staff at the College will agree to abide by an AUP consistent across the Trust as part of their employment contract with the College (Appendix 1)
    c. Inappropriate use of the College's ICT system by students will be dealt with in accordance with the policy on Managing Behaviour through Rewards, Recognition and Positive Behaviour with the addition that it will be reported to the Online Safety Coordinator and copied to ICT Administration Support.
    Students will have their student login suspended, normally for a period of 14 days. AUP breaches will be recorded on SIMS Behaviour Manager as appropriate and a letter will usually be sent to parents, along with a new copy of the AUP for the student and parent/carer to sign. ICT access will be reinstated following the return of this AUP and the expiry of their suspension period.
    d. Inappropriate use of the College's ICT system by staff will be dealt with in accordance with grievance and disciplinary procedures (Section E of Staff Handbook).

Revised February 2016

Glossary of Terms

AUP – Acceptable Use Policy

CEOP – Child Exploitation and Online Protection Centre – www.ceop.police.uk

ICT – Information and Communications Technology

FTP – File Transfer Protocol

SIMS – School Information Management System

Social Networking – Websites such as Facebook or Twitter where users set up a personal profile and can message/chat with other users as well as upload material.

Appendix 1 - Staff Acceptable Use Policy (LF Trust)

Staff

Acceptable Use Policy (AUP)

This Acceptable Use Policy (AUP) applies to all Landau Forte Trust Staff employed in any of its central functions or Academies, including any temporary staff, associate staff, contractors, and visitors. The agreement applies to anyone accessing any part of the Landau Forte Trust systems whether onsite, or remotely from offsite.

As an employee/representative of Landau Forte Trust, you may have access to confidential and potentially sensitive information stored on the Trust network and systems. You may also have access to other electronic devices supplied to you by the Trust such as Laptops, Personal Digital Assistants (PDAs), and Smartphone/phones. You are responsible for any Trust equipment in your care including your user account and email, their contents and activity.

You should not under any circumstances:

- Access, store, distribute or print material from any medium which:
  a) may bring the Trust name into disrepute
  b) may compromise the safety of the Trust, its students or employees
  c) may be deemed offensive to your colleagues
  d) is considered to be illegal or inappropriate
- Install, copy, or bring into Trust software which is not correctly licensed for use.
- Allow anyone else to access your user account, email, intranet or internet services.
- Allow anyone else to know your password.
- Change any computer files that do not belong to you or that you do not have access to.
- Plagiarise work without acknowledging the source.

The Trust provides fast and reliable internet and email access to all staff which has a filtering service that attempts to block illegal, unwanted and potentially offensive material. Content which passes these filters is not necessarily deemed to be acceptable by Landau Forte Trust. Therefore, if you find any material which is inappropriate, offensive, illegal, controversial, or which is generally not suitable for staff or students to access, please contact the Systems Support Team who will attempt to block it.

You are allowed to use the Landau Forte Internet and Email system for personal use outside of contracted hours, but you should not:

- § Use the Internet or Email for any illegal or inappropriate purpose.
- § Engage in any online activity that may compromise your professional responsibilities.
- § Use impolite or abusive language.
- § Violate the rules of common sense and etiquette.
- § Send or receive copyright materials without permission.
- § Use the Internet to bring into Landau Forte, in any form, materials that would be unacceptable on paper.

You are allowed to use the Landau Forte Internet and Email system for personal use, but you must:

- § Only use the approved, secure email system for any Landau Forte business.
- § Only use the approved Landau Forte email, VLE or other approved communication systems with students or parents/carers, and only communicate with them on appropriate business.
- § Ensure that any private social networking sites/blogs/twitter accounts etc that you create, or actively contribute to, are not confused with your professional role. NB: access to Social Networks, e.g. Facebook, and personal email accounts is prohibited during your contracted hours.

If you need to use personal equipment on the Trust network (e.g. you are an MFL Assistant and need your own laptop as it is in your native language) please ensure that:

- § It does not contain material which is deemed unsuitable or inappropriate, as outlined above.
- § It has an antivirus checker installed, with the latest updates applied.
- § Use personal digital cameras or camera phones for taking and transferring images of students or staff without permission, and also not store images at home without permission.

Landau Forte Trust reserves the right to:

- View user's email.
- View user's internet usage/history and where necessary, interrogate and analyse that information.
- View any files stored in user areas or shared areas on the Trust Network.
- View any material on Trust owned equipment *and to take appropriate action if these files contravene the policy as detailed above.*

I understand that all Internet usage and network usage is logged and that this information could be made available to the Senior Leadership Team upon request. I understand that failure to comply with this agreement could lead to disciplinary action.

Appendix 2 - Formal College signature

<Name in Calibri pt 16>

<Job Title in Calibri pt 11>

Landau Forte College Derby
Fox Street, Derby, DE1 2LF

Tel 01332 204040
Fax 01332 371867

www.landau-forte.org.uk

Appendix 3 - External e-mail disclaimer

Appendix 4 - Student Acceptable Use Policy

ICT USER ACCOUNT ACCEPTABLE USE POLICY

A. YOUR COLLEGE ICT USER ACCOUNT

1. As a Landau Forte College student, you have your own College ICT User Account on the College network. This facility enables you to electronically store and retrieve your work and importantly to access learning resources from both inside and outside of the College. To retain your ICT User Account you must comply with the terms of this policy.

2. YOU are responsible for the content of your user area and you MUST NOT under any circumstances:

    a. Allow anyone else to access your user account, e-mail or internet link or to know your password.
    b. Use anyone else's user account and/or password.
    c. Leave your login session unattended.
    d. Change any computer files that do not belong to you or that you do not have access to.
    e. Play or download games, music or other inappropriate or sensitive material.
    f. Plagiarise (copy) others' work without acknowledging the source.
    g. Bring hardware or software into College which has not been authorised for use.

B. INTERNET AND ELECTRONIC MAIL

1. The internet and e-mail facilities are excellent resources and you are encouraged to use these in a constructive and positive way which will help both your learning and your communication with other users.

2. The College provides fast and reliable internet and electronic mail access with connections to other computer systems located all over the world. Therefore users must understand that the College cannot control the content of the information on these systems but we do use a filtering service which attempts to block illegal, unwanted and potentially offensive material. The College does not condone or approve of the use of such materials and will use its best endeavours to prevent access to all such inappropriate materials by using a filtered service and by regularly checking User Accounts including their Internet activity. Content which passes these filters cannot necessarily be assumed to be acceptable. If you find material which is inappropriate, offensive, illegal, controversial, or which is unsuitable, you should contact the Systems Management Team, or a Tutor, as soon as possible who will attempt to block access to and from that site.

3. When using your account you have a responsibility to help to protect yourself, other students and staff as well as the reputation of your College. Therefore YOU MUST NOT:

    a. Use the internet or e-Mail for any illegal or inappropriate purpose.
    b. Use impolite or abusive language.
    c. Use unauthorised web mail sites. (You are provided with e-mail access from College).
    d. Violate the rules of common sense and etiquette.
    e. Send or receive copyright materials without permission.
    f. Use the internet or e-mail system to bring into College, in any form, materials that would be unacceptable on paper.
    g. Attempt to circumvent the e-mail and internet filters implemented by the College e.g. by use of proxy server.

4. Landau Forte College reserves the right to view your electronic mail, internet history and files stored in your user area, elsewhere on the College network or held on a personal storage device (including lap top computer or USB key)or mobile technology (including smartphone, tablet etc.) that is brought into College and is or has been connected to the network.

5. If your behaviour and/or the contents of your College ICT User Account contravene this Acceptable Use Policy then appropriate action will be taken in accordance with the College policy *Managing Behaviour through Rewards and Action.*

STUDENT AGREEMENT

I have read the ICT User Account Acceptable Use Policy and I understand that my activity on the College ICT network will be monitored. Monitoring will include:

    a. All files stored anywhere on the College network plus any that are held on a personal storage device (including lap top computer or USB key) or mobile technology (including smartphone, tablet etc.) that is brought into College and is or has been connected to the network.
    b. My Internet Activity
    c. E-mails sent or received.

I understand that a breach of the Acceptable Use Policy may result both in the loss of privileges on the network and in further action being taken against me in line with the College policy *Managing Behaviour through Rewards and Action*

Signed by Student: _____

Signed by Parent/Carer: _____

First Name: _____ Last Name: _____ PT: _____

Date: _____ Year Group _____

WHEN SIGNED THIS DOCUMENT SHOULD BE RETURNED TO THE COLLEGE

Appendix 5 – Secure Password Policy

SECURE PASSWORD POLICY

This policy is complementary to other College policies, particularly the On-line Safety Awareness and Education policy.

Context

Landau Forte College Derby is committed to the use of the Internet and other expanding technologies within education. Under our duty of care, Landau Forte College Derby has the responsibility to ensure that all users of technology understand the risks and are able to take proactive measures to safeguard themselves.

This policy addresses the issues surrounding the safe and secure use of the College's ICT system.

Purpose

To ensure that all student, staff, governors and third parties that use ICT at the College are aware of the dangers of using an insecure password and are educated on how best to ensure that any passwords used are secure.

This policy applies to all students, staff, governors and third parties that have any form of ICT account requiring a password on the College network including but not limited to a domain account and email account.

Secure Password Requirements

Landau Forte College Derby operates a secure password policy which forces users of the College ICT system to choose a password meeting strict requirements. All passwords must be at least 8 characters and include at least 3 of the following 4 types of characters;

1. Lower Case Characters (e.g. abc)
2. Upper Case Characters (e.g. ABC)
3. Numbers (e.g 123)
4. Special Characters / Symbols (e.g. !?@)

The previous 10 used passwords cannot be used when changing a password.

Secure Password Guidance

In order to aid the creation of a secure password, the following guidance is issued:

- Think of a phrase that means something to you. Use the first letters of each word, changing some letters to upper case, and adding some numbers.
  For example: *My favourite football team is Wolves = MffTiW12*

- Don’t just use one password for all systems that you use. Make passwords unique by adding a unique identifier for each system that you use.
  For example: *MffTiW12Am for Amazon or MffTiW12Tw for Twitter*

- Don’t include any personal details which may be readily known to others
  For example: *your street name, your birthday, names of pets, similar*

- Avoid using dictionary words, as these are easy to guess and can quickly be cracked using computer software.

- Don’t rely on simple alphanumeric substitutions to strengthen a password
  For example: *0 for O and 1 for i*

- Don’t use common sequences of numbers or letters
  For example: *1234567 or abcdefg*

Maintaining a Secure Password

It is important to ensure that it is kept secure once it has been set. The following guidance is issued in order to ensure that passwords are kept secure:

- Protect passwords by making sure that nobody is looking over your shoulder when you enter them

- Never write down your password or store them on any unencrypted computer system

- Do not email or otherwise communicate your password to anyone

- Ask IT support to change your password if you have reason to believe that someone else knows it

- Be aware of ‘phishing’, when hackers create a copy of a legitimate website (such as an online banking website) and send an email to users asking them to update their details using the link provided.

Reporting Security Incidents

All security incidents should be reported immediately to IT support. These incidents include occasions when:

- A password may have been accidentally revealed

- It is suspected that access has been gained to a system by an unauthorised person

Appendix 5 – Managing Personal data - Guidelines for staff

MANAGING PERSONAL DATA – GUIDELINES FOR STAFF

Staff are reminded of their responsibilities with respect to managing the security and sensitivity of personal data.

1. Personal information should not be uploaded to any cloud storage providers. Secure storage facilities are provided in College.

2. If you are required to email personal information outside of the College, it should be secured with a password, which should be sent separately. You should take adequate steps to ensure that the information is being sent to the correct recipient and only the data required is being sent.

3. Personal information that needs to be transported using a memory stick, should be encrypted / password protected. If you are unable to use an encrypted / password protected memory stick, the files themselves should be password protected.

4. Personal information should not be taken off-site unless necessary.

5. Personal information should not be transferred onto a personal device. It should remain on College devices only.

6. Personal information should only be stored for as long as it is required. If you no longer have a need to store certain information, you should delete it.

7. Personal information stored on the College network should be stored in a location where only required personnel can access it. Saving personal information in a location where it can be accessed by unauthorised users is a breach of data protection laws.

8. Photos of students should not be shared without the permission of the student (This information is stored in SIMS). Photos of students under 16 should not be used alongside their full name. The sharing of student photographs should only be done via official channels ie. College official Website / Social Media / Newslink etc.