newcollaborative Learning Trust

Student IT Acceptable Usage Policy

Version 4

This policy applies to all NCLT institutions.

Thorpe Hesley Primary School – Where Children Grow

To be the best that we can be – Redscope Primary School

Anston Greenlands Primary School – Love to Learn

DINNINGTON HIGH SCHOOL

Wingfield Academy

Achieving Excellence – Brinsworth Academy

newcollege Doncaster

newcollege Bradford

newcollege Pontefract

CONTENTS

1.0 Introduction

The purpose of this policy is to outline the acceptable use of IT resources by students. Students at New Collaborative Learning Trust rely on information technology (IT) to support their learning in and beyond the classroom. This Acceptable Use Policy (AUP) provides a set of rules for using the IT resources at the Trust and protects the users and property. It is the responsibility of every user to know these guidelines and to conduct their activities accordingly.

These rules are in place to protect all users and the NCLT IT systems and infrastructure, data and property, inappropriate use could expose the network to risks including virus attacks, compromise of network systems and services.

2.0 Acceptable Use Policy

By using the Trust IT services in any of its school/college/primary, you are agreeing to and are bound by the terms set out in this document and agree that all Trust devices and systems can be monitored for security and safety reasons, the Trust will not be responsible for any loss of data as a result of the system or students mistakes in using the system. Use of any information obtained via the network is at the student's own risk.

2.1 Secondary School and College Students

I agree that I will:

- be responsible for my ICT activity and so will not give my username and password to anybody else and not attempt to log on using another person's username and password or access another person's files.
- not attempt to gain unauthorised access to any part of the Trust network that is not available from my personal logon, either via the network or the Internet.
- not connect any personal equipment to the Trust network without prior consent of the IT Manager.
- not attempt to use or load programs, files, tools or shortcuts to gain access to either the hard drive of the Trust workstations or any other part of the network and not attempt to store any computer software on the Trust network.
- not attempt to store any computer software on the Trust network that the Trust has no license for.
- not attempt to store any free software on the Trust network without prior consent of the IT Manager.
- immediately report any instance where I have inadvertently gained access to restricted areas to a member of staff.
- only visit websites, which are appropriate to my work at the time and only use the Internet to help me with my work when using a Trust computer.
- not visit websites that contain unsuitable material. If I am unsure if a site is suitable, I will ask a member of staff.
- be responsible when setting a new password, minimum of 10 characters, include the following uppercase characters (A through to Z) lowercase (a through to z) Numbers (0 through 9), Special characters (example _, -, =, + ,!, @, *, /,)
- not open unknown links and files in the interest of security/cyber-attacks.
- save my work and log off properly after I have finished with the computer
- not access or create any material that may cause upset to others.

- ask IT support If I am unsure about opening or downloading any attachments or contents of an email.
- not use portable media (like memory sticks) on the network without gaining permission from my teacher.
- not attempt to set-up or use any proxy by-pass software, in order to by-pass the Trust Internet filter.
- no anyone whom I have made contact with on the Internet without discussing this first with my parents/carers
- not take information from the Internet and pass it off as my own work. If any work is found to have been plagiarised it will be given a Zero mark.
- report any misuse of the Internet immediately to a member of staff.
- be responsible in my use of email. I will not include in an email any material that is inappropriate. I will not use offensive or threatening language in my emails or in any other communication on the Internet. I understand that any email going out from the Trust will carry the Trust address and so represents the Trust.
- always keep my personal details private.
- only copy pictures or text into my area on the network. I will not download any other type of file, for example software, games, screen savers, Music, Films, etc.
- use the Wireless or Guest Wireless network to the same responsible ways listed in this policy (depending which school or college site you are at)
- not abuse the Printing and Copying services, all printing, copying and scanning is monitored and logged for abuse of use over and above normal practice.
- not post any defamatory remarks relating to Trust Staff or Students to any Public Web sites either inside or outside the Trust, including Facebook, Twitter, Google +, and other websites where public users have access to view posts.
- report to a teacher any concerns about inappropriate information or conduct on social media sites which are offensive; demeaning, harassment (including sexual harassment), victimisation or bullying.
- all users accessing the bring your own devices wireless network do so under the agreement of Trust ICT Acceptable Use Policy and agree to adhere to conditions set out in this policy documentation. Students choosing to bring personal devices into the Trust do so at their own risk. (if applicable to your site)
- treat Trust IT equipment with care and attention and accept that if I deliberately damage deface or vandalise IT equipment I will be charged the full cost and will be placed on contract, further action may be forthcoming in accordance with the behaviour policy of the school/college.

I accept that:

- The IT systems are provided to allow me to perform my work, whilst the Trust provides a reasonable level of privacy.
- All usage of the Trusts IT systems remains the property of the Trust; this may be stored data, emails images etc.
- All Trust devices and systems can be monitored for security and safety reasons.
- The Trust may monitor any aspects of its computer systems that are made available to any user and may also monitor intercept and/or record any communications made, including telephones email or internet communications. The Trust will ensure compliance in line with the Regulation of Investigatory Powers Act (RIPA) 2000, and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

2.2 Primary Specific, for EYFS, KS1 and KS2 pupils. This is how we stay safe when we use computers:

- I will not have my own email address (This is specific to EYFS and KS1)
- I will only go on the internet using my own username and password.
- I will not try and get to any websites that the school has blocked access to.
- I will only use memory sticks with permission from my teacher.
- I will not install any software on school computers.
- I will return any school-owned ICT equipment to my teacher when I have finished using it.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not eat or drink while using school-owned ICT equipment.
- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not give away any of my personal details (full name, age, date of birth, ~~sex~~ gender, address etc.) or the personal details of other users in school, over the internet. This includes photography or video images of me, other pupils or members of staff.
- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.
- If I see any hurtful comments about the school, staff or pupils. I will take screenshots for evidence and report to the e-safety coordinator.
- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.
- I will not publish anything online, e.g., images or pictures, without asking my teacher.
- I will only use my class email address to contact people I know or those agreed by my teacher.
- There are times I can ask a teacher or suitable adult if I am allowed to use a computer / tablet.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will not use my own personal devices (mobile phones / USB devices etc) in school time, at breakfast, after school clubs or school events (e.g. a concert or disco). If I bring a mobile phone into school, I will hand it to a responsible adult to look after.
- ~~I~~ will not upload any photographs or videos taken on school premises or at school clubs or events to any website.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I know that if I break these rules I might not be allowed to use a computer / tablet.

3.0 Criminal Conduct/Radicalisation and Extremism Test

3.1 Criminal Conduct/Radicalisation and Extremism related to the use of the Internet or email are covered by law, and by Trust policy and are unacceptable. These will be regarded by the Trust as constituting misconduct and any student involved will be subject to disciplinary action up to expulsion. These include: terrorist activities, on-line stalking, grooming, internet luring, soliciting of children by computer, defamation, retention of offensive screen savers, fraud, software theft, damage to Trust systems, retention of other people's personal details/information, drug-related activities, or any other illegal activity. The Terrorism Act (2006) outlaws web posting of material that encourages or endorses terrorist acts, even terrorist acts carried out in the past. Sections of the Terrorism Act also create a risk of prosecution for those who transmit material of this nature, including transmitting this material electronically.

3.2 Again, visits to websites related to jihadism/other forms of terrorism/ downloading of material issued by Jihadis /other terrorist groups (even from open-access sites) may be subject to monitoring by the police.

3.3 In addition, Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on the Trust to have, in the exercise of its functions, due regard to the need to prevent people from being drawn into terrorism. This means that the Trust will place an appropriate amount of weight on the need to prevent people being drawn into terrorism in the application of this policy.

4.0 Social Media Advice and Policy

4.1 Please refer to the Social Media Policy located on the Trust website which clearly outlines the disciplinary procedures for students who use social media inappropriately.

5.0 Data Protection

5.1 Please refer to the Trust Data Protection Policy and Personal Data Breach Policy.

6.0 Further updates to this policy

6.1 This policy may be updated or modified at any time should the college deem it necessary. Sections of the acceptable usage policy will be displayed on your computer and must be accepted from time to time before web usage is allowed. The college reserves the right to administer these rules in a fair and unbiased way, which may

result in a student's access to either the internet or the college network being removed or other appropriate sanction being taken.

Equality Impact Assessment (EIA)

The completion of this document is a requirement for all existing and proposed New Collaborative Learning Trust (NCLT) policies, major procedures, practices and plans (hereafter referred to as policies) as well as whenever looking at policy updates.

The Equality Act 2010 sets out our legal duty to undertake equality analysis of all trust/college policies. Completion of this EIA is the first step in meeting this duty. Please send the completed EIA (together with a copy of the related policy/draft policy document) to the Trust Director for Human Resources who will review the document and may refer to the Equality and Diversity Committee as necessary to advise on any follow up action that might be required.

Completion of the Equality Impact Assessment is part of the Specific Equality Duties (SED) required of the trust. Over arching the specific duties is the General Equality Duty (GED) required of everyone. Please bear the GED and SED in mind when undertaking this audit.

General Equality Duty

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.
- Advance equality of opportunity between people who share a protected characteristic and those who do not.
- Foster good relations between people who share a protected characteristic and those who do not.

Specific Equality Duties Relevant to EIA are to provide:

- Sufficient information to demonstrate compliance with the general duties; including effects policies have on people.
- Evidence that analysis of this information has been undertaken.
- Details of information considered during analysis.
- Details of engagement (consultation) that has taken place.

Protected Characteristics are:

- Age
- Disability
- Gender Reassignment
- Marriage/Civil Partnership
- Pregnancy/Maternity Leave
- Race
- Religion or Belief
- ~~Sex~~ Gender
- Sexual Orientation

Audit Prompt	Response
Name of policy	Acceptable Use Policy
Author of document:	Jodie Richardson
Responsible Senior Manager:	Jodie Richardson

Briefly describe the aims, objectives and purpose of the policy.	To ensure the guidelines of the AUP are followed to protect users, property and network.
Who does the policy apply to: • Staff • Learners (please indicate which groups) • Members of the general public (please specify)	Students
Will the policy affect members of the target audience equally? If no, please indicate the specific groups targeted by the policy. In targeting the policy at a specific group of people will members of other groups be disadvantaged? If yes, how will this be addressed? What information has been gathered about the diversity of the target audience? Attach details of information considered. How has this diversity been taken into account in writing the policy?	All affected equally, no groups disadvantaged, the policy is applied fairly.
Does this policy contain visual images? If yes, are these technical or cultural in nature? If cultural, do they reflect diversity? If yes, please indicate how.	No
Please indicate how this policy supports the trust/college in its General Equality Duty to: • Eliminate unlawful discrimination, harassment and victimisation (A). • Advance equality of opportunity between people who share a protected characteristic and those who do not (B). • Foster good relations between people who share a protected characteristic and those who do not (C).	A By providing clear guidelines that students must follow whilst accessing NCLT network B the policy does not do this C the policy does not do this
Please indicate any negative impacts identified in relation to the protected characteristics listed below, or how you have arrived at the view that there are not negative impacts in relation to these characteristics: Age	No impacts identified

Disability Gender Reassignment Marriage/Civil Partnership Pregnancy/Maternity Leave Race Religion or Belief Sex Sexual Orientation	
Is the policy free from discrimination on the grounds of: • Additional Learning Needs • Economic Needs • Social Needs	YES
Please indicate who the policy has been considered by and/or who has been consulted about the policy. Where applicable include: • Staff/student consultative groups • Trade unions • Equality and Diversity, Health and Safety and Safeguarding Committee • Other committees/working groups (specify) • Senior Management Team • Trust Executive Team • Board of Directors • External group / Advisory group (specify)	TET
Can you identify any further consultations that might be necessary to ensure no adverse impact? If yes, please specify.	No
Can you identify any differential or adverse impact the policy might have that is not already recorded? If yes, please specify.	No
How would you assess the overall impact of this policy on equality? Please circle.	High / Medium / Low

Please record who this audit has been completed by (if by committee/work group please indicate and get lead person to sign off):	Name : Jodie Richardson Job Title : Trust Director of IT Date : 08/10/2024

Where necessary the policy will be reviewed by the Equality and Diversity Committee who may require additional information to fully analyse the impact of the policy and any actions/changes needed to address any negative impacts identified.