Greenhead College Corporation

ONLINE SAFETY POLICY

Reviewed June 2022

Table of Contents

Acknowledgement

This policy is based on an original document '**YHGfL Guidance for Creating an eSafety Policy'** written by Yorkshire and Humberside Grid for Learning. It has been adapted by Kirklees Learning Service for use in Kirklees Colleges and now Greenhead College.

1. Introduction

This Online Safety policy recognises our commitment to keeping staff and students safe online and acknowledges its part in the College's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep students safe when using technology. We believe the whole College community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with students.

As part of our commitment to Online Safety we also recognise our obligation to implement a range of security measures to protect the College network and facilities from attack, compromise, and inappropriate use and to protect College data and other information assets from loss or inappropriate use.

The scope of policy

- This policy applies to the whole College community including the Senior Leadership Team (SLT), Governing Body (GB), all staff employed directly or indirectly by the College, visitors, and all students.
- The SLT and College governors will ensure that any relevant or new legislation that may impact upon the provision for online safety within College will be reflected within this policy.

The person in College taking on the role of Online Safety Lead is Usman Anwar (Designated Safeguarding Lead (DSL)).

The person in College with responsibility for the IT Network is Paddy Diamond (Director of Information Services).

The Governor with an overview of Online Safety matters is Michelle Lister

The following groups were consulted during the creation of this Online Safety policy: Staff, students, and Governors.

Implementation of the policy

- The SLT will ensure all members of staff are aware of the contents of the Online Safety Policy and the use of any new technology.
- All staff, students, occasional and external users of our ICT equipment will agree to the Internet Code of Conduct.
- All amendments will be published, and awareness sessions will be held for all members of the College community.
- Online safety will be taught as part of the curriculum in an age-appropriate way to all students.

- The Online Safety Policy will be made available to parents, carers, and others via the website.

2. Responsibilities of the College Community

We believe that online safety is the responsibility of the whole College community and that everyone has their part to play in ensuring all members of the community can benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The senior leadership team accepts the following responsibilities:

- The Principal will take ultimate responsibility for the online safety of the College community.
- Identify a person (the Online Safety Lead) to take day to day responsibility for online safety; provide them with training; monitor and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system.
- Ensure policies and procedures are in place to ensure the integrity of the College's information and data assets.
- Ensure liaison with the governors.
- Develop and promote an online safety culture within the College community.
- Ensure that all staff, students, and other users agree to the Internet Code of Conduct and that new staff have online safety included as part of their induction procedures.
- Make appropriate resources, training, and support available to all members of the College community to ensure they can carry out their roles effectively regarding online safety.
- Ensure that the correct procedures are followed should an online safety incident occur in College and review incidents to see if further action is required.

Responsibilities of the Online Safety Lead

- Promote an awareness and commitment to online safety throughout the College.
- Be the first point of contact in College on all online safety matters.
- Take day to day responsibility for online safety within the College.
- Lead the College online safety team and/or liaise with technical staff on online safety issues.
- Create and maintain online safety policies and procedures.

- Develop an understanding of current online safety issues, guidance, and appropriate legislation.
- Ensure delivery of an appropriate level of training in online safety issues.
- Ensure that online safety education is embedded across the curriculum.
- Ensure that online safety is promoted to parents and carers.
- Ensure that any person who is not a member of College staff, who makes use of the College ICT equipment in any context, is made aware of the Internet Code of Conduct.
- Liaise with the Local Authority, the Local Safeguarding Children Board, and other relevant agencies as appropriate.
- Monitor and report on online safety issues to SLT and the Safeguarding Governor as appropriate.
- Ensure that staff and students know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident.
- To promote the positive use of modern technologies and the internet.
- To ensure that the College Online Safety Policy and Internet Code of Conduct are reviewed at prearranged time intervals.

Responsibilities of all Staff

- Read, understand, and help promote the College's online safety policies and guidance.
- Read, understand, and adhere to the staff acceptable use of IT.
- Take responsibility for ensuring the safety of sensitive College data and information.
- Develop and maintain an awareness of current online safety issues, legislation, and guidance relevant to their work.
- Always maintain a professional level of conduct in their personal use of technology.
- Ensure that all digital communication with students is on a professional level and only through College based systems, **NEVER** through personal email, text, mobile phone social network or other online medium.
- Embed online safety messages in learning activities where appropriate.
- Supervise students carefully when engaged in learning activities involving technology.
- Ensure that students are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable.
- Report all online safety incidents which occur to a College safeguarding coordinator.

- Respect the feelings, rights, values, and intellectual property of others in their use of technology in College and at home.

Additional Responsibilities of Technical Staff

- Support the College in providing a safe technical infrastructure to support learning and teaching.
- Ensure appropriate technical steps are in place to safeguard the security of the College ICT system, sensitive data, and information. Review these regularly to ensure they are up to date.
- Ensure that provision exists for misuse detection and malicious attack.
- At the request of the SLT conduct occasional checks on files, folders, email, and other digital content to ensure that the Internet Code of Conduct is being followed.
- Report any online safety related issues that come to their attention to a College safeguarding coordinator.
- Ensure that suitable access arrangements are in place for any external users of the College's ICT equipment.
- Liaise with the Local Authority and others on online safety issues.
- Document all technical procedures and review them for accuracy at appropriate intervals.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Responsibilities of Students

- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of College.
- Ensure they respect the feelings, rights, values, and intellectual property of others in their use of technology in College and at home.
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening.
- Report all online safety incidents to appropriate members of staff.
- Discuss online safety issues with family and friends in an open and honest way.
- To know, understand and follow College policies on the use of mobile phones, digital cameras, and handheld devices.
- To know, understand and follow College policies regarding online bullying.

Responsibilities of Parents and Carers

- Help and support the College in promoting online safety.
- Read, understand, and promote the Internet Code of Conduct with their children.
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Consult with the College if they have any concerns about their child's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to, and help promote the College's online safety policies and guidance as part of the College's overarching safeguarding procedures.
- Support the work of the College in promoting and ensuring safe and responsible use of technology in and out of College, including encouraging parents to become engaged in online safety awareness.
- To have an overview of how the College IT infrastructure provides safe access to the internet and the steps the College takes to protect personal and sensitive data.
- Ensure appropriate funding and resources are available for the College to implement their online safety strategy.

Responsibilities of the Designated Safeguarding Lead

- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.
- Be aware of and understand the risks to young people from online activities such as grooming for Child Sexual Exploitation (CSE), sexting and online bullying and the risks of radicalisation in line with Prevent Duty and guidance. Government Guidance on Prevent: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf
- Raise awareness of the issues which may arise for vulnerable students in the College's approach to online safety ensuring that staff know the correct child protection procedures to follow.

Responsibility of any external users of the College systems

- Take responsibility for liaising with the College on appropriate use of the College's IT equipment and internet, including providing an appropriate level of supervision where required.

3. Internet Code of Conduct

As a user of the College's computer facilities, you must agree to use it within certain constraints. This code outlines the most important points which you are expected to follow.

- There is to be NO USE OF FREE E-MAIL sites (hotmail/gmail etc.) whatsoever. You are only permitted to use the e-mail facilities offered by the College. Your e-mail address is <studentnumber>@greenhead.ac.uk
- Absolutely no access to chat or social networking sites is allowed.
- Recreational use of the Internet is only permitted outside the normal College hours, although access to the Internet will still be filtered in line with College policy.
- No student is allowed to make use of another student's username, either with or without their permission.
- Any private printing must be paid for at the Finance Office.
- E-mail facilities must not be used for any abusive or obscene purposes.
- Pornographic and other similar types of sites are blocked - any attempted access to this type of site is forbidden.
- Printing of pages from the Internet must be done with due attention to the volume of paper used. Make sure you are going to use the pages before you print them. Ensure you collect any printed pages from the printer.
- The College's proxy server carries out various checks on Internet pages so that their content can be verified and logged. The log files will show student users who have broken the above code.
- Any students who find that they are unable to follow the above points will have their access to the College Internet facilities removed.

4. Training

Technology use changes at a fast pace, and we recognise the importance of regular staff training. The Online Safety Lead will attend training updates when available. All College staff will receive regular updates on risks to students online from the Online Safety Lead.

5. Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our College community lies in effective education. We know that the internet and other technologies are embedded in our students' lives, not just in College but outside as well, and we believe we have a duty to help prepare our students to benefit safely from the opportunities that these present.

We will teach students how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and students will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We will discuss, remind, or raise relevant online safety messages with students routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind students about the responsibilities to which they have agreed.

Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

6. How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this, we will offer opportunities for finding out more information through the College newsletter and website.

We will ask all parents to discuss the Internet Code of Conduct with their child.

We request our parents to support the College in applying the Online Safety Policy.

7. Managing and safeguarding IT systems

The College will ensure that access to the College IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up to date. Staff have virus protection installed on all laptops used for College activity.

All administrator or master passwords for College IT systems are kept secure and available to at least two members of staff e.g., Principal and member of technical support.

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named individuals e.g., a member of technical support.

We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on College provided laptops.

Filtering Internet access

Teachers are encouraged to check out websites they wish to use prior to lessons for the suitability of content.

Access to College systems

The College decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the College who may be granted a temporary log in.

All users are provided with a log in appropriate to their role in College. Students are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and College and in creating secure passwords.

Access to personal, private, or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information.

Remote access to College systems is covered by specific agreements and is never allowed to unauthorized third-party users.

Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, College management information system).

- We provide all staff with a unique, individually named user account and password for access to IT equipment, email, and information systems available within College.

- All students have a unique, individually named user account and password for access to IT equipment and information systems available within College.

- All staff and students have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.

- The College maintains a log of all accesses by users and of their activities while using the system to track any online safety incidents.

8. Using the Internet

We provide the internet to

- Support curriculum development in all subjects.
- Support the professional work of staff as an essential professional tool.
- Enhance the College's management information and business administration systems.
- Enable electronic communication and the exchange of curriculum and administration data with the LA, examination boards and others.

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the College IT systems or a College provided laptop or device and that such activity can be monitored and checked.

All users of the College IT or electronic equipment must always abide by the relevant Internet Code of Conduct (ICC), whether working in a supervised activity or working independently,

Students and staff are informed about the actions to take if inappropriate material is discovered, and this is supported by notices in classrooms and around College.

Using email

Email is regarded as an essential means of communication and the College provides all members of the College community with an e-mail account for College based communication. Communication by email between staff, students and parents will only be made using the College email account and should be professional and related to College matters only. Email messages on College business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the College is maintained. There are systems in place for storing relevant electronic communications which take place between College and parents.

Use of the College email system is monitored and checked.

It is the personal responsibility of the email account holder to keep their password secure.

Under no circumstances will staff contact students, parents or conduct any College business using a personal email address.

Responsible use of personal web mail accounts on College systems is permitted outside teaching hours.

Publishing content online

E.g., using the College website, Learning Platform, blogs, wikis, podcasts, social network sites

College website:

The College maintains editorial responsibility for any College initiated web site or publishing online to ensure that the content is accurate, and the quality of presentation is maintained. The College maintains the integrity of the College web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the College address, email, and telephone number. Contact details for staff published are College provided.

Identities of students are always protected.

Online material published outside the College:

Staff and students are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside College as they are in College.

Material published by students, governors and staff in a social context which is considered to bring the College into disrepute or considered harmful to, or harassment of another student or member of the College community will be considered a breach of College discipline and treated accordingly.

Using images, video, and sound

We recognise that many aspects of the curriculum can be enhanced using multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Students are taught safe and responsible behaviour when creating, using, and storing digital images, video, and sound.

The College allows you to take photographs in College of your own child or children only. This is subject to you recognising the need to be sensitive to other people, not causing interruption or disruption to concerts, performances, and events. Please note that if publishing photographs of your own children on websites or social networking sites, the name of the College should not be added alongside any such images.

Parents/carers should not publish or upload any images of other students onto any websites or social networking sites. This is to respect the rights of other parents/carers not to have images of their children published or distributed without their knowledge or consent.

Using video conferencing, web cameras and other online meetings

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow students to link up with people in other locations and see and hear each other. We ensure that staff and students take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Students do not operate video conferencing equipment, answer calls, or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

Please refer to the College's 'Student Code of Conduct for Zoom Classroom sessions' policy and 'Student Code of Conduct for Microsoft Teams Classroom Sessions" for further, specific details.

Using mobile phones

Use of mobile phones by students is covered in the Mobile Phone Policy.

During lesson time we expect all mobile phones belonging to staff to be switched off unless there is a specific agreement for this not to be the case.

Using mobile devices

We recognise that the multimedia and communication facilities provided by mobile devices (e.g., iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities for students. However, their use in lesson time will be with permission from the teacher and within clearly defined boundaries.

Students are taught to use them responsibly.

Using personal devices

Staff and students are allowed to use their own personal devices to access College resources and systems.

All personal devices used to access College resources and systems must adhere to the following requirements:

- All devices must be running an up to date and currently supported version of the operating system that is receiving regular security updates.
- All applications on the device must by up to date and currently supported.
- Operating systems and software must be set to auto update.
- Staff and students using medical devices should update any operating systems and software on their device prior to accessing College Wi-Fi.

- Where applicable, software firewalls, antivirus and anti-malware software must be installed and up to date.
- The device must be protected by a strong password/lock screen that have been changed from the default password.
- The device must not be left unlocked while logged into College systems or while accessing College resources.
- Access to College resources must only be used via official applications from the respective device App Store. These include Microsoft Office applications such as Outlook and OneDrive and official browsers such as Google Chrome, Firefox, Internet Explorer, Edge, Opera, Safari etc.
- The device must not be jailbroken, rooted etc., or have unofficial or "cracked" applications “sideloaded” on it.

All staff must provide the following information about the personal devices that they use to access College resources and systems.

- The device type - desktop, laptop, mobile, tablet etc.
- Model.
- The Operating system version.

Using other technologies

The College will keep abreast of new technologies and evaluate both the benefits for learning and teaching and the risks from an online safety point of view.

We will regularly review the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by students.

Staff or students using a technology not specifically mentioned in this policy, or a personal device, whether connected to the College network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

9. Protecting College data and information

College recognises their obligation to safeguard staff and students’ sensitive and personal data including that which is stored and transmitted electronically. The College is a registered Data Controller under the Data Protection Act 1998 / Data Protection (Charges and Information) Regulations 2018. We regularly review our practices and procedures to ensure that they meet this basic obligation, and we always comply with the requirements of that registration. All access to personal or sensitive information owned by the College will be controlled appropriately through technical and non-technical access controls.

Students are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended.
- Staff are provided with appropriate levels of access to the College management information system holding student data. Passwords are not shared, and administrator passwords are kept securely.
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside College.
- All devices taken off site, e.g., laptops, tablets, removable media, or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.
- When we dispose of old computers and other equipment, we take due regard for destroying information which may be held on them.
- We follow Kirklees procedures for transmitting data securely and sensitive data is not sent via email unless encrypted.
- Remote access to computers is by authorised personnel only.
- We have full back up and recovery procedures in place for College data.
- Where sensitive staff or student data is shared with other people who have a right to see the information, for example governors or Kirklees officers, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies.

Management of assets

Details of all College-owned hardware and software are recorded in an inventory.

All redundant IT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

10. Dealing with online safety incidents

Any incidents where students do not follow the Internet Code of Conduct will be dealt with following the College's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious online safety incident concerning students or staff, they will inform a College safeguarding coordinator who will then respond in the most appropriate manner.

Instances of **online bullying** will be taken very seriously by the College and dealt with using the College's anti-bullying procedures. College recognises that staff as well as students may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the College network, or create an information security risk, will be referred to the College's Online Safety Lead and technical support and appropriate advice sought, and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures, or guidance. If the action breaches College policy, then appropriate sanctions will be applied. The College will decide if parents need to be informed if there is a risk that student data has been lost.

College reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about child protection or the discovery of indecent images on the computer, then the procedures outlined in the College Safeguarding Policy will be followed.

Dealing with complaints and breaches of conduct by students:

- Any complaints or breaches of conduct will be dealt with promptly.
- Responsibility for handling serious incidents will be given to a senior member of staff.
- Parents and the student will work in partnership with staff to resolve any issues arising.
- Restorative practice will be used to support the victims.
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately.
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, or violent.
- continuing to send or post material regarded as harassment or of a bullying nature after being warned.
- staff using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites).

The following activities are likely to result in disciplinary action:

- any online activity by a member of the College community which is likely to adversely impact on the reputation of the College.
- accessing inappropriate or illegal content accidentally and failing to report this.
- inappropriate use of personal technologies (e.g., mobile phones) at College or in lessons
- sharing files which are not legitimately obtained e.g., music files from a file sharing site.
- using College or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the College into disrepute.
- attempting to circumvent College filtering, monitoring, or other security systems.
- circulation of commercial, advertising or ‘chain’ emails or messages.
- revealing the personal information (including digital images, videos, and text) of others by electronic means (e.g., sending of messages, creating online content) without permission.
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content).
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act 1998.

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g., as part of planned curriculum activity or by a system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time.
- accessing non-educational websites (e.g., gaming or shopping websites) during lesson time.
- sharing a username and password with others or allowing another person to log in using your account.
- accessing College IT systems with someone else's username and password.
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else.

Author:	*Designated Safeguarding Lead* *Director of Information Services*
Date drafted:	*April 2016*
Date accepted by the Corporation:	*May 2016*
Date of next review:	*June 2024*

"This policy has been impact assessed to ensure it complies with all aspects of Equality and Diversity. Members are reassured that this policy is compliant with current equality legislation".