

# Norton College E-Safety policy

Member of Staff Responsible: Headteacher/Business Manager/Designated Senior Lead

Governors' Committee: Full/Education/Business

Approved on: 13/10/20

Review Date: October 2021

Signed off by:

Chair of Governors: Karron Young

Date: 13/10/20

## 1. Introduction

Norton College understands that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the College recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The College has adopted this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The College is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented controls to reduce any harmful risks.

This policy will be updated as necessary to reflect best practice, or amendments made to legislation, and shall be reviewed every 12 months from 18/10/2020

“Users” – Any person including staff, students or external “Network Manager” – Senior ICT Technical Lead person “Staff” – Any person directly employed by the College “Pupil” – Any pupil currently registered to the College.

## 2. Legal framework

2.1. This policy has due regard to the following legislation, including, but not limited to:

2.1.1. Human Rights Act 1998

2.1.2. General Data Protection Regulation 2018

2.1.3. Freedom of Information Act 2000

2.1.4. Regulation of Investigatory Powers Act 2000

2.1.5. Safeguarding Vulnerable Groups Act 2006

2.1.6. Education and Inspections Act 2006

2.1.7. Computer Misuse Act 1990 amended by the Police and Justice Act 2006

2.1.8. Communications Act 2003

2.1.9. Protection of Children Act 1978

2.1.10. Protection from Harassment Act 1997

2.2. This policy also has regard to the following statutory guidance:

2.2.1. DfE (2019) ‘Keeping children safe in education’

2.3. This policy may be used in conjunction with other College policies and procedures, as appropriate.

## 3. Consideration when using the internet

3.1. When accessing the internet, individuals are especially vulnerable to several risks which may be physically and emotionally harmful, including:

- 3.1.1. Access to illegal, harmful or inappropriate images
- 3.1.2. Cyber bullying
- 3.1.3. Access to, or loss of, personal information
- 3.1.4. Access to unsuitable online videos or games
- 3.1.5. Loss of personal images
- 3.1.6. Inappropriate communication with others
- 3.1.7. Illegal downloading of files
- 3.1.8. Exposure to explicit or harmful content, e.g. involving radicalisation
- 3.1.9. Plagiarism and copyright infringement
- 3.1.10. Sharing the personal information of others without the individual's consent or knowledge

## 4. Roles and responsibilities

4.1. It is the responsibility of all users to ensure that the internet, both inside and outside of the College, is used in an appropriate and legal manner. If any user are witnesses to or believe that ANY illegal or harmful activities have or are taking place, they **MUST** inform an appropriate member of staff immediately.

4.2. The network manager is responsible for the implementation and day to day management of the safety systems and software used within the College and managing any issues that may arise. This includes ensuring that appropriate filtering is in place for all users and that this is up to date.

4.3. The network manager will provide technical support and advice to members of staff as required and will support any wider College CPD.

4.4. The Head Teacher will ensure there is a system in place which monitors and supports the network manager, whose role is to work with the Designated Safeguarding Lead (DSL) to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

4.5. The College will ensure that all members of staff are aware of the procedure when reporting e- safety incidents.

4.6. The network manager and DSL will carry out regular reviews of internet usage data by all users and address any concerns as they arise. Proactive monitoring **MUST** take place and the appropriate staff member **MUST** be alerted directly and automatically of any incidents.

4.7. Cyber bullying incidents will be reported in accordance with the College Anti-Bullying Policy.

4.8. Teachers are responsible for ensuring that e-safety is embedded in the curriculum and safe internet access is promoted at all times.

4.9. All staff and pupils will ensure they understand and adhere to The College's Acceptable Use Policy, which they must agree to, prior to logging onto the College IT systems. The College will keep a log of acceptance and this must be updated as changes occur.

4.10. All pupils MUST be made aware of their responsibilities regarding the use of College-based ICT systems and equipment, including their expected behavior.

## 5. E-safety education

### 5.1. Educating pupils:

5.1.1. The College will regularly update pupils to make sure they are aware of the safe use of new technology both inside and outside of the College.

5.1.2. Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.

5.1.3. Pupils will be taught to acknowledge information they access online, to avoid copyright infringement and/or plagiarism.

5.1.4. Pupils are instructed to report any suspicious use of the internet and digital devices to a member of staff.

5.1.5. The College will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

### 5.2. Educating staff:

5.2.1. E-safety training opportunities MUST be available to all staff members, including whole College activities and CPD accredited training courses where appropriate.

5.2.2. All staff will undergo e-safety training including cyber security on an annual basis to ensure they are aware of current issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.

5.2.3. All staff will undergo an annual "Skills Audit" by the College that will identify individual CPD needs of staff.

5.2.4. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

5.2.5. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

5.2.6. Any new staff are required to undergo online safety and awareness training as part of their induction programme, ensuring they fully understand this E-Safety Policy.

5.2.7. The network manager will act as the first point of contact for staff requiring general e- safety advice. Safeguarding issues or concerns MUST be processed using the College Safeguarding processes.

## 6. E-safety control measures

### 6.1. Internet access:

6.1.1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with the Colleges Acceptable Use Policy.

6.1.2. A record will be kept by the College of all pupils who have been granted internet access.

6.1.3. All users in key stage 3 and above will be provided with usernames and passwords and must keep these confidential to avoid any other pupils using their login details.

6.1.4. Management systems may be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

6.1.5. Keeping Children Safe in Education compliant filtering systems **MUST** be in place and in use to reduce any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

6.1.6. Any requests by staff for websites to be added or removed from the filtering list must be logged and first authorised by the Head Teacher.

6.1.7. All College systems **MUST** be protected by up-to-date anti-virus software.

6.1.8. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

*These accounts **MUST** be assigned to a single user and logged to ensure that in the event of any abusive, illegal, or behavioral matter can be investigated and allow the investigating office to identify a single individual.*

6.1.9. Staff are able to use the internet for lawful and appropriate personal use during out-of- College hours, as well as break and lunch times. Please Note: All internet activity on College devices will leave a digital footprint. Any person choosing to use College devices for personal reasons is giving permission for Norton College to have this data until such time that the digital footprint is purged.

6.1.10. Personal use will only be monitored by the network manager, HR or safeguarding staff for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

6.1.11. Inappropriate internet access by a member of staff may result in the staff member being restricted. Please see the process outlined in section 8.4 of this policy.

## 7. Social networking:

7.1. Access to social networking sites will be filtered as appropriate.

7.2. Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Head Teacher.

7.3. Staff are not permitted to communicate with pupils over personal social networking sites and are reminded to alter their privacy settings accordingly.

7.4. Staff are not permitted to publish comments about the College which may affect its reputation.

7.6. Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This MUST be discussed with the Head Teacher prior to accessing the social media site and explicit permission provided.

## 8. Published content on the College website and images:

8.1. The Head Teacher will be responsible for the overall content of their College website and will ensure the content is appropriate and accurate.

8.2. Contact details on the College website will include the phone number, email and address of the College.

8.3. Images and full names of pupils, or any content that may easily identify a pupil, must follow the College policies relating to the Data Protection Act 2018.

8.4. Pupils are not permitted to take or publish photos of others without permission from the individual.

8.5. Staff are able to take pictures, though they must do so in accordance with College policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.

8.6. Any member of staff that is representing the College online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the College, or any information that may affect its reputability.

## 9. Mobile devices and hand-held computers:

9.1. The Head Teacher may authorise the use of mobile devices for a pupil and staff where it is seen to be for safety, precautionary or educational use.

9.2. If permitted pupils and staff will access the College Bring You Own Device (BYOD) Wi-Fi system using their personal mobile devices and hand-held computers providing the user and/or device meets the Colleges criteria. Internet access will be monitored for any inappropriate use by the network manager when using these on the College premises.

9.3. Pupils and staff are not permitted to access the Colleges general use Wi-Fi system at any time using their personal devices.

9.4. Staff are permitted to use hand-held computers which have been provided by the College, though internet access will be monitored for any inappropriate use by the network manager and/or DSL when using these on the College premises.

9.5. Using the Colleges devices or network to send inappropriate messages or images is prohibited.

9.6. Mobile devices will not be used to take images or videos of pupils or staff.

9.7. The College will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

## 10. Network security:

10.1. Please see the College's "eSecurity Policy" for additional information.

10.2. Each user will be provided with an account name and password. Users will be permitted to change passwords as required and must change them as a minimum every 2 months.

10.3. Passwords have a minimum length of 8 characters including a minimum of 1 number and 1 uppercase character.

10.4. Passwords MUST NOT be shared with other users, if a user becomes aware of another users log on details the user MUST inform a member of staff immediately.

10.5. No “Generic” or “Multi-User” accounts will be created or used by any User unless the accounts are managed in the following way:

10.5.1. The account is assigned to a single individual and the name and time is logged including start and end time.

10.5.2. Once the activity has ended an appropriate member of staff will change the password to something that meets the minimum requirements (this can easily be done by pressing several random keys in the Notepad (or similar) program then copy and paste this into the password field but do NOT save the document)

10.5.3. The change of password is also logged entering user and time of change.

## 11. Cyber bullying

11.1. This section must be reviewed alongside the College “Anti-Bullying Policy”

11.2. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

11.3. The College recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

11.4. The College will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

11.5. The College will commit to creating a learning and teaching environment which is free from harassment and bullying, for all staff and pupils.

11.6. The Head Teacher will decide whether it is appropriate to notify the police or other appropriate parties regarding the action taken against a pupil or staff member.

## 12. Reporting misuse

12.1. The College will clearly define what is classed as inappropriate behavior in the Acceptable Use Policy, ensuring all pupils and staff members are aware of what behavior is expected of them.

12.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e- safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

12.3. Misuse by pupils:

12.3.1. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Head Teacher.

12.3.2. Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be willfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.

12.3.3. Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the Head Teacher and will be issued once the pupil is on the College premises.

12.3.4. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with the “Child Protection and Safeguarding Policy” and reported to the Designated Safeguarding Lead (DSL).

#### 12.4. Misuse by staff:

12.4.1. Any misuse of the internet by a member of staff should be immediately reported to the Head Teacher.

12.4.2. The Head Teacher will deal with such incidents in accordance with the “Allegations of Abuse Against Staff Policy” and may decide to take disciplinary action against the member of staff.

12.4.3. The Head Teacher will decide whether it is appropriate to notify the police of the action taken against a member of staff.

#### 12.5. Use of illegal material:

12.5.1. In the event that illegal material is found on any of the College networks, or evidence suggest that illegal material has been accessed, the College may contact external parties for further investigation and support. Where appropriate police will be contacted.

12.5.2. Incidents will be immediately reported to the “Internet Watch Foundation” and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

12.5.3. If a child protection incident is suspected, the Colleges child protection procedure will be followed – the DSL and Head Teacher will be informed, and the police contacted.