



Online Safety Policy

Member of staff responsible:

Deputy Head (Pupils)

Last reviewed October 2022
Next review due October 2023

This policy requires Governor approval

Definition of Terms

AUP	Acceptable Use Policy
BYOD	Bring Your Own Device
CEOP	Child Exploitation and Online Protection Centre
College	Ashville College, including the Boarding Houses, Ashville Acorns Pre-Prep (including Reception), Prep School, Senior School and Sixth Form
Cyberbullying	Bullying that takes place over digital devices like cell phones, computers, and tablets
College Network	Any IT system or service that is owned or managed by the College. This includes but is not limited to things such as Microsoft365, PASS, ISAMS, SOCS, Operoo
DPA	Data Protection Act 2018 and the General Regulations on Data Protection
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessments
DSL	Designated Safeguarding Lead
EYFS	Early Years Foundation Stage
FOI	Freedom of Information
Fortigate	Software designed to filter internet access across the College
GDPR	General Data Protection Regulation
Governors	Directors of Ashville College Trustee Limited
Head	Head of the College
ICO	Information Commissioners Office - UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
ICT	Information and Communications Technology
INSET	In Service Training Day
KS1	Key Stage 1
LADO	Local Authority Designated Officer
PC	Personal Computer

PCI	Payment Card Industry
Pupils	Pupils who attend the College including pupils in the Early Years Foundation Stage (EYFS)
PSHE	Personal, Social and Health Education
SMT	Senior Management Team (Senior School)
Staff	Any member of the staff employed by the College in either a teaching or non-teaching role, members of the Governing Body and Volunteers working within the College
USB	An interface that enables communication between devices i.e. a computer and a flash drive, digital camera, keyboards and printers

Policies to be read in conjunction with this policy

- Acceptable Use Policy
- Anti-bullying Policy
- Child Protection Policy
- College Behaviour Policy
- Data Protection Policy
- Relationships and Sex Education Policy
- Searching Pupils and their Possessions Policy
- Whistleblowing Policy

Other documents to be read in conjunction with this policy

- Images of Pupils – Taking, Storing and Using
- Procedure on Removal from the College
- Staff Code of Conduct

The following guidance should also be referred to when relevant

- [Keeping Children Safe in Education](#) (September 2022)
- [North Yorkshire Safeguarding Children Partnership](#)
- Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People – UKCCIS Guidance
- [Teaching Online Safety in Schools](#)

1 Introduction

- 1.1 The College is a caring community based on Methodist values and, as such, the well-being of each of its members is a prime concern.
- 1.2 Information and Communication Technology (ICT) has transformed the process of teaching and learning in the College. It is a crucial component of every academic subject and is also taught as a subject in its own right. All pupils are taught how to research on the internet and to evaluate sources. They are instructed in the

importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution.

- 1.3 ICT provides unrivalled opportunities for enhanced learning and business practices, but these new technologies can put young people and staff at risk both within and outside the College. Some of the dangers they may face include;
 - 1.3.1 **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
 - 1.3.2 **contact:** being subjected to harmful online interaction with other users; for example: child to child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
 - 1.3.3 **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
 - 1.3.4 **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils or staff are at risk, please report it to the [Anti-Phishing Working Group](#).

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy is used in conjunction with other College Policies as listed above.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

Pupils are therefore taught how to stay safe in this environment and how to mitigate risk, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

- 1.4 When using the Internet to enter or share information it is important that we consider what data we are making available and how this can be viewed by others. Most social networking sites have privacy settings which can and should be used to limit the audience who can access this information.
- 1.5 The Data Protection Act of 2018 was brought in to protect the rights and privacy of individuals and to ensure that data about them is not processed without their consent where necessary. It covers data held in all formats. The Data Protection Act of 2018 is the UK implementation of the GDPR.

2 Child Protection

- 2.1 The College recognises that internet safety is a child protection and general safeguarding issue. The DSL, one of the Deputy DSL and the IT Manager have been trained in safety issues involved with the misuse of the internet and other mobile electronic devices. They work to promote a culture of responsible use of technology

that is consistent with the ethos of the College. All of the staff, especially those with pastoral responsibilities, receive training in online safety issues.

- 2.2 The three schools each have a programme of online safety which ensures that all year groups in the College are educated, in an age-appropriate way, in the risks and reasons why they need to behave responsibly online. The Head of Pre-Prep, Head of Prep and the Deputy Head (Pupils) are responsible for overseeing the programme in the College.

3 Scope of the Policy

- 3.1 This policy applies to all staff, pupils, parents/carers, visitors and community users who have access to and are users of College ICT systems and services, both in and out of the College.
- 3.2 The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published College Behaviour Policy.
- 3.3 The College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of College.

4 Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the College:

4.1 Governors

Governors are responsible for the approval of the Online Safety Policy, and for reviewing the effectiveness of the policy ensuring it is disseminated to the wider College community. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

The role of the Governing Body does include ensuring that the statutory requirements of Keeping Children Safe in Education September 2022 are complied with. In relation to online safety this includes:

- 4.1.1 ensuring that as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach;
- 4.1.2 ensuring that pupils are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through PSHE;

- 4.1.3 as schools increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. A school needs to ensure the appropriateness of any filters, monitoring and security systems which will be informed in part by the risk assessment required by the Prevent Duty to ensure that children are safe from terrorist and extremist material whilst accessing the material in school, including by establishing appropriate levels of filtering but being careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

The role of the Safeguarding Governor includes:

- 4.1.4 regular meetings with the Online Safety Lead, the DSL;
- 4.1.5 attendance at e-Safety Team meetings (by one of the Safeguarding Governors);
- 4.1.6 regular monitoring of online safety incident logs and responding appropriately to identified needs;
- 4.1.7 reporting to Full Governor's Committee each term.

4.2 The Head

The Head should ensure:

- 4.2.1 the Governors comply with the online safety aspects of Keeping Children Safe in Education (September 2022) documentation;
- 4.2.2 the safety (including online safety) of all members of the College community;
- 4.2.3 effective and regular training about online safety is provided for the whole College community and a log is kept of the staff who complete the training;
- 4.2.4 Governors are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety education, health and safety or child protection;
- 4.2.5 effective communication with parents/carers about safe practices when using online technology's and support them in talking to their children about these issues;
- 4.2.6 effective filtering, monitoring and security systems are set up;
- 4.2.7 there are effective procedures in place in the event of an online safety allegation which are known and understood by all members of staff;
- 4.2.8 establishing and reviewing the College online safety policy and documents and making them available on the College website;
- 4.2.9 the College's DSL should be trained in online safety issues and be aware of the potential for serious child protection issues that could arise through the use of ICT.
- 4.2.10 That the staff involved in online safety systems and procedures for the College have sufficient capacity to manage them.

4.3 The Senior Leadership Team

The Senior Leadership Team should:

- 4.3.1 liaising with staff, ICT Technical staff, Online Safety Governor, ELT and partner agencies on all issues related to online safety;
- 4.3.2 ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- 4.3.3 providing training and advice for staff and keeping a log of staff who complete training about online issues;
- 4.3.4 keep a log of staff, pupils and families who have signed the Acceptable Use Policy (AUP) for the safe use of technology;
- 4.3.5 receive and respond to reports of online safety incidents and create a log of incidents and outcomes to inform future online safety developments;
- 4.3.6 Coordinating and reviewing online safety education programme in the College (or working in partnership with the Personal, Social, Health, Education (PSHE) and/or Computing lead).

4.4 Online Safety Lead

The Online Safety Lead;

- 4.4.1 leads the e-safety team;
- 4.4.2 takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the College online safety policy/documents;
- 4.4.3 ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- 4.4.4 provides/organises training and advice for staff on online safety matters;
- 4.4.5 liaises with the College ICT technical staff;
- 4.4.6 receives reports of online safety incidents and creates a log of incidents to inform future online safety developments;
- 4.4.7 meets termly with the Safeguarding Governor to discuss current issues and review incident logs and filtering;
- 4.4.8 reports regularly to the ELT;
- 4.4.9 attends the relevant committee of the Governing Body.

4.5 Chief Information Officer and Technical Staff

The IT Manager and Technical Staff are responsible for ensuring;

- 4.5.1 that the College's technical infrastructure is secure and is not open to misuse or malicious attack and meets requirements for filtering and monitoring and any other relevant cyber security legislation;
- 4.5.2 that the College meets required online safety technical requirements including any requirements of 'Keeping Children Safe in Education' (September 2022), PCI Compliance and the GDPR that may apply;
- 4.5.3 that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed in line with current best practice guidance;

- 4.5.4 that they keep up to date with online safety technical information ~~and~~, cyber security and data protection best practice in order to effectively carry out their online safety role and to inform and update others as relevant;
- 4.5.5 that the use of the network/internet/ remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Lead/ Deputy Head (Operations/ Deputy Head (Pupils)/ Head of Lower School/Head of Upper School/Head of Sixth Form/ Deputy Head of Prep School for investigation/ action/sanction;
- 4.5.6 that monitoring software/systems are implemented and updated as agreed in College policies.
- 4.5.7 That reporting system meet the requirements of Keeping Children Safe in Education (September 2022)

4.6 All Staff

In addition to understanding the elements covered in the Staff Acceptable Use Policy (AUP), all staff are responsible for ensuring that;

- 4.6.1 they have an up to date awareness of online safety matters and of the current College Online Safety Policy and practices;
- 4.6.2 they attend the training provided by the College about online safety and all new staff receive online safety training as part of their induction programme, ensuring that they fully understand the College online safety policy, Acceptable Usage and Child Protection Policies;
- 4.6.3 they have read, understood and signed the College Staff Acceptable Usage Policy AUP;
- 4.6.4 they do not 'be-friend' any pupil or pupil family member on social media in a social context whilst the pupils are at the College or for five years after they have left;
- 4.6.5 online safety issues are embedded in all aspects of the curriculum and other College activities;
- 4.6.6 pupils understand and follow the College's Online Safety and acceptable usage policies;
- 4.6.7 pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- 4.6.8 they monitor ICT activity in lessons, extracurricular and extended College activities;
- 4.6.9 in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- 4.6.10 all staff should be aware that emails can be part of Freedom of Information and subject access requests so all correspondence needs to be professional, courteous and respectful;
- 4.6.11 if confidential information/information under the data protection act is being sent by email it must be sent through the secure email system, e.g. the Egress system.
- 4.6.12 Data protection procedures and policies must not prevent the sharing of safeguarding information if it were to jeopardise an investigation or response to an incident.

4.7 Designated Safeguarding Lead

The DSL should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from;

- 4.7.1 sharing of personal data;
- 4.7.2 access to illegal/inappropriate materials;
- 4.7.3 inappropriate online contact with adults/strangers;
- 4.7.4 potential or actual incidents of grooming;
- 4.7.5 cyber-bullying.

4.8 E-Safety Team

The e-Safety Team provides a consultative group that has wide representation from the College community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the e-Safety Team will assist the Online Safety Lead (or another relevant person) with;

- 4.8.1 the production/review/monitoring of the College Online Safety Policy/ documents;
- 4.8.2 mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression;
- 4.8.3 monitoring network/internet/incident logs related to safeguarding issues;
- 4.8.4 consulting stakeholders – including parents/carers and the pupils about the online safety provision.

4.9 Pupils

Pupils:

- 4.9.1 are responsible for using the College ICT systems in accordance with the Pupil Acceptable Use Policy, which they are expected to 'agree to' before being given access to College systems;
- 4.9.2 have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- 4.9.3 need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- 4.9.4 will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying;
- 4.9.5 should understand the importance of adopting good online safety practice when using digital technologies out of College and realise that the College's Online Safety Policy covers their actions out of College, if related to their membership of the College.

4.10 Pupils – EYFS Setting

EYFS has a duty to provide children with quality internet access as part of their learning.

- 4.10.1 Internet access is tailored expressly for educational use and includes appropriate filtering.
- 4.10.2 Pupils in EYFS learn appropriate internet use.
- 4.10.3 Staff guide pupils in online activities that will support their learning journeys.
- 4.10.4 Staff are responsible for ensuring that material accessed by the children is appropriate.
- 4.10.5 Children do not access the internet unattended.
- 4.10.6 Internet safety in EYFS depends on staff, parents, carers and visitors taking responsibility for the use of internet and other communication technologies such as mobile phones. (See Images of Pupils - Taking, Storing and Using Policy.)
- 4.10.7 Filters are in place to limit internet access and to monitor effectiveness.
- 4.10.8 Permission from parents or carers for featuring their child on the website is requested when each child starts College and parents/carers wishes are followed at all times.
- 4.10.9 Online learning journals are secure, and parents can only access their own child's journal.

4.11 Parents/Guardians

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents are also responsible for monitoring their children's internet use and for ensuring that their children are not involved in any incidents of cyber-bullying.

It is recognised that not all parents and carers may feel equipped to protect their child(ren) when they use electronic equipment at home hence the College organises occasions and age-appropriate information evenings for parents/guardians when a specialist offers advice about the potential hazards of this exploding technology, and the practical steps that parents/guardians can take to minimise the potential dangers to their child(ren) without curbing their natural enthusiasm.

The College seeks to work closely with parents and guardians in promoting a culture of online safety. The College will always contact parents/guardians if there are any worries about a child or young person's behaviour in this area, and parents/guardians are encouraged to share any worries with us.

Parents and guardians will be encouraged to support the College in promoting good online safety practice and to follow guidelines on the appropriate use of;

- 4.11.1 digital and video images taken at College events;
- 4.11.2 access to parents' sections of the website on online pupil records;
- 4.11.3 their children's personal devices in the College.

Parents and guardians will be responsible for:

- 4.11.4 endorsing (by signature) the Pupil Acceptable Usage Policy within the Prep School;
- 4.11.5 Endorsing that they do not use social media to criticise or make inappropriate comments about the College or an individual member of staff as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/guardian, they have any concerns about anything which happens in the College then please contact the College directly.

5 Policy Statements

5.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the College's online safety provision. Children and young people need the help and support of the College to recognise and avoid online safety risks and build their resilience.

Online safety education will be provided in the following ways:

- 5.1.1 A planned online safety programme will be provided as part of ICT/PSHE and will be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College.
- 5.1.2 A range of safeguarding issues are considered as part of the online safety education: keeping their personal information private, healthy relationships on and off line, grooming, sending inappropriate images and the consequences of this, gaming, gambling, radicalisation and how to recognise the signs and keep themselves safe.
- 5.1.3 Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- 5.1.4 Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- 5.1.5 Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- 5.1.6 Pupils will be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and out of College.
- 5.1.7 Staff should act as good role models in their use of ICT, the internet and mobile devices.
- 5.1.8 Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- 5.1.9 It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant

designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

5.2 Education – Parents/Guardians

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure how to respond.

The College will therefore seek to provide information and awareness to parents and guardians through;

- 5.2.1 specific parent information sessions;
- 5.2.2 letters, newsletters, website, the parent portal;
- 5.2.3 providing a list of relevant links/resources (see **Appendix 2**)

5.3 Education and Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- 5.3.1 A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly:
- 5.3.2 It is expected that some staff will identify online safety as a training need within their personal appraisal process:
- 5.3.3 All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the College Online Safety Policy and Acceptable Use Agreements:
- 5.3.4 The Online Safety Lead/Director of Digital Innovation and Communication will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations:
- 5.3.5 This Online Safety Policy and its updates will be presented to and discussed by staff in staff/INSET days:
- 5.3.6 The Online Safety Lead/Director of Digital Learning will provide advice/guidance/training to individuals as required.

5.4 Training – Governors

Governors will be offered online safety training through participation in College training/information sessions for staff or parents.

6 ICT Acceptable Use Policy

Online safety is a whole College responsibility, and all staff and pupils are required to adhere to an ICT Acceptable Use Policy, which incorporates the following guidelines in age appropriate ways:

6.1 Treating others with Respect

- 6.1.1 The College expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact. They should always follow the College's Code of Conduct for Pupils, Prep School Rules, Senior School and Sixth form rules which are discussed with pupils in the Prep School and copies of which are displayed in the schools.
- 6.1.2 The College expects a degree of formality in communications between staff and pupils and would not in normal circumstances expect them to communicate with each other by text or mobile phone.
- 6.1.3 Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The College is strongly committed to promoting equal opportunities for all, regardless of race, gender, religious affiliation, cultural background, gender orientation, disability or Special Educational Needs.

6.2 Cyberbullying

- 6.2.1 Cyberbullying is a particularly pernicious form of bullying, because it can be pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The College's Anti-bullying Policy sets out preventative measures and the procedures that will be followed where cases of bullying are discovered.
- 6.2.2 Proper supervision of pupils plays an important part in creating a safe ICT environment at College; but everyone needs to learn how to stay safe out of College.
- 6.2.3 Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and they should not be afraid to report the matter.

6.3 Keeping the College's Network Safe

- 6.3.1 Certain sites are blocked by the College's filtering system and the system monitors all use of the network and the IT Manager will oversee the checking of this on a regular basis.
- 6.3.2 The system also monitors e-mail traffic and blocks SPAM and certain attachments.
- 6.3.3 All pupils from Year 3 upwards are issued with their own personal College e-mail address. Access is via a personal LOGIN, which is password protected. Guidance is given on the reasons for always logging off and for keeping all passwords secure.
- 6.3.4 There is strong anti-malware protection on the College network, which has been installed by IT Support.

6.4 Passwords are an Important Element of Keeping the Users of the College ICT System Safe

6.4.1 Use of Passwords for Staff and Governors

- Passwords or encryption keys should not be recorded on paper or in an unprotected file.

- Passwords should be changed at least every 60 days.
- Users should not use the same password on multiple systems or attempt to 'synchronise' passwords across systems.

6.4.2 Use of Passwords for Pupils

- Should only let College staff know their in-school passwords.
- Should not share their password with another pupil/sibling.
- Inform staff immediately if passwords are traced or forgotten.

Acceptable Use Policies for ICT usage are given to staff and pupils. Copies of this are displayed in classrooms around the College and in the Boarding Houses. The College will impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices (see Appendix 4 and Appendix 5).

7 Technical – Infrastructure/Equipment, Filtering/Monitoring and Reporting

7.1 The College will be responsible for ensuring that the College infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- 7.1.1 College technical systems will be managed in ways that ensure that the College meets recommended technical requirements:
- 7.1.2 There will be regular reviews and audits of the safety and security of College technical systems:
- 7.1.3 Servers, wireless systems and cabling are securely located, and physical access is restricted:
- 7.1.4 All users will have clearly defined access rights to College ICT systems:
- 7.1.5 All users will be identifiable to filtering and monitoring systems
- 7.1.6 All users will be provided with a username and secure password by the IT Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every 60 days:
- 7.1.7 The 'administrator' passwords and private encryption keys for the College system, used by the IT Manager (or other person) must also be available to the Head or other nominated senior leader and kept in a secure place (e.g. College safe):
- 7.1.8 Users are responsible for the security of their username and password, must not allow other users to access the system using their log on details and must immediately report any suspicion or evidence that there is a breach of security:
- 7.1.9 The IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations:
- 7.1.10 Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered through 'Fortigate'. Content lists are regularly updated, and internet use is logged and regularly monitored:
- 7.1.11 The Internet filtering should also ensure that children are safe from terrorist and extremist material when accessing the internet:

- 7.1.12 The internet filtering will be age appropriate and also consider the needs of individual roles within the College. The College will seek to ensure 'over-blocking' is kept to a minimum.
- 7.1.13 The College provides enhanced user-level filtering through the use of 'a Fortigate Web Filter'. In the event that the IT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head (or other nominated senior leader, excluding the IT Manager):
- 7.1.14 Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager and the relevant Deputy Head. If the request is agreed, this action will be recorded:
- 7.1.15 Reports on internet usage, safeguarding risk and other trends will be regularly delivered to the appropriate staff.
- 7.1.16 College IT Support staff passively monitor and record the activity of users on the College ICT systems and users are made aware of this in the Acceptable Use Policy:
- 7.1.17 Remote management tools are used by staff to control workstations and view user's activity:
- 7.1.18 An appropriate system is in place for users to report any actual/potential technical incident/online safety incident to the Chief Information Officer (or other relevant person) – see **Appendix 3**:
- 7.1.19 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and individual workstations are protected by up to date EDR software:
- 7.1.20 An agreed policy is in place for the provision of temporary access of 'guests' (e.g. trainee teachers, supply teachers, visitors) onto the College system:
- 7.1.21 An agreed policy is in place regarding the extent of personal use that users (staff/pupils) are allowed on College devices that may be used out of College:
- 7.1.22 An agreed policy is in place that forbids staff from installing programmes on College workstations/portable devices:
- 7.1.23 An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on College workstations/portable devices:
- 7.1.24 Personal data cannot be sent over the internet to non-College systems or taken off the College site unless agreed by the Data Protection Officer.

8 Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- 8.1 In lessons where internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- 8.2 Where pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites that the pupils visit. Searches

should be logged on the Colleges web filter and checked for their appropriateness and if they pose a safeguarding risk.

- 8.3 It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager can temporarily remove these sites from the filtered list for the period of study. Any request to do so, should be recorded with clear reasons for the need.
- 8.4 Pupils will be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of the information.
- 8.5 Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

9 Bring Your Own Device (BYOD)

- 9.1 The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by the College of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of online safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments and users should refer to the Acceptable Use Policy as well as Parental Information on Mobile Devices, but the following provide a brief overview of the key points:

- 9.1.1 The College has a set of clear expectations and responsibilities for all users:
- 9.1.2 The College adheres to the Data Protection Act principles:
- 9.1.3 All users are provided with and accept the Acceptable Use Policy:
- 9.1.4 All network systems are secure and access for users is differentiated:
- 9.1.5 Where possible these devices will be covered by the College's normal filtering systems while being used on the premises:
- 9.1.6 All users will use their username and password and keep this safe:
- 9.1.7 Pupils receive training and guidance on the use of personal devices:
- 9.1.8 Regular audits and monitoring of usage will take place to ensure compliance:
- 9.1.9 Any device loss, theft, change of ownership of the device will be reported.

10 Social Media and Telephone Communication

- 10.1 The College IT Manager and IT Support staff have a key role in maintaining a safe technical infrastructure at the College and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the College system and data and for training our teaching and support staff in the use of ICT. They monitor the use of the internet and e-mails and will report any observed inappropriate usage to the appropriate senior manager. It is the responsibility of all staff to report any inappropriate usage to the IT Manager. Access to sites of inappropriate content is blocked from the College network, as is access to social media such as Facebook during the College day. (Boarders have access to Facebook in the evenings, but this is monitored by staff in the boarding houses on a regular basis.) Other exceptions

include departments that have a legitimate need to engage on social media platforms. These users will receive appropriate training on the safe use of social media sites.

10.2 Appropriate Use of Email

- 10.2.1 Digital communications with pupils and parents/guardians should be on a professional level and only carried out using official College systems.
- 10.2.2 The College's email service should be accessed via the provided web-based interface by default.
- 10.2.3 Under no circumstances should staff or governors contact pupils, parents/guardians or conduct any College business using personal email addresses.
- 10.2.4 College email is not to be used for personal use.
- 10.2.5 All staff should be aware that emails can be part of Freedom of Information and subject access requests so all correspondence needs to be professional, courteous and respectful.

10.3 Appropriate use of Mobile Phones

- 10.3.1 College mobile phones only should be used to contact parents/carers/pupils when on College business with pupils off site. Staff should not use personal mobile devices and under no circumstances should a pupil or parent/guardian be given a member of staff's personal mobile number.
- 10.3.2 Staff should not be using personal mobile phones.
- 10.3.3 Visitors will be asked not to use their mobile phone whilst on site with any pupil presence due to all mobile phones containing a camera.
- 10.3.4 Pupils should adhere to the rules and guidelines set out in the College Behaviour Policy/Mobile Phone Guidance regarding mobile phone use in College.
- 10.3.5 All pupils will be required to put their phone/interactive watch in a lockable container at the start of any PE lesson.
- 10.3.6 All pupils will be required to put their phones/interactive watches in a lockable container at the start of any examinations.

10.4 Appropriate Use of Social Networking Sites

- 10.4.1 Staff should not access social networking sites on College equipment in school or at home that have not been pre-approved by the College.
- 10.4.2 Staff users and governors should not refer to any member of staff, the governing body, pupils, parents/carers, the College or any other member of the College community on any social networking site or blog in a derogatory way.
- 10.4.3 Pupils will not be allowed on social networking sites on College equipment that have not been pre-approved whether in College or at home. At home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.
- 10.4.4 Pupils/Parents/guardians should be aware the College will investigate misuse of social networking if it impacts on the well-being of other pupils or members of the College community.
- 10.4.5 Parents/guardians and pupils will be informed that they do not use social media to criticise or make inappropriate comments about the College, an

- individual member of staff or another pupil as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/guardian, they have any concerns about anything which happens in College they should contact a member of staff.
- 10.4.6 If inappropriate comments are placed on social networking sites about the College or College staff then advice would be sought from the relevant agencies, including the police if necessary.
- 10.4.7 Pupils will be taught about online safety when using social networking sites.

11 Use of Digital and Video Images – Photographic, Video

- 11.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, pupils and parents/guardians need to be aware of the risks associated with publishing digital images on the internet. Those images may provide avenues for cyberbullying to take place; digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The same issues can arise with digital recordings made of individuals.
- 11.2 The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
- 11.2.1 When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- 11.2.2 Written permission from parents or guardians will be obtained before photographs of pupils are published on the College website/social media/local press;
- 11.2.3 In accordance with guidance from the Information Commissioner's Office, parents/guardians are welcome to take videos and digital images of their children at College events for their own personal use (as such use as not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/guardians comment on any activities involving other pupils in the digital/video images;
- 11.2.4 Staff are allowed to take digital/video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Those images should only be taken on, or processed thereafter, College equipment, the personal equipment of staff should not be used for such purposes;
- 11.2.5 Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute;
- 11.2.6 Pupils should not take, use, share, publish or distribute images (for example, video or photographs) of staff or pupils without their permission:

- 11.2.7 Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- 11.2.8 Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs;
- 11.2.9 A pupil's work can only be published with the permission of the pupil and parents or guardians;
- 11.2.10 The College will liaise with external providers and places visited on school trips to ensure they do not take photographs and use the images on their website/social media without permission of a member of staff from the College.

11.3 The Terms and Conditions that parents sign includes a section as follows:

You consent to us making use of information relating to your child (including photographs and video recordings), and (where appropriate) relating to you, whilst your child is at the College and after they have left for the purposes of:

- (i) managing relationships between the College and current pupils/parents and fulfilling our obligations under the contract with you;*
- (ii) promoting the College to prospective pupils/parents;*
- (iii) publicising the College's activities; and*
- (iv) communicating with the College community and the body of former pupils.*

In respect of (ii), (iii) and (iv), this includes use of such information by the College in/on the College's prospectus (in whatever format or medium it is produced/made available), the College's website(s) and (where appropriate) the College's social media channels.

If you do not want your child's photograph or image to appear in any of the College's promotional material you must make sure your child knows this and must give notice to the Head, this notice will be acknowledged by the College.

11.4 Staff need to be mindful of the possible child protection issues associated with the possession of images of children and as such they are required to adhere to the following policy:

- 11.4.1 All images and video taken of individual pupils or groups of pupils must be uploaded **as soon as possible** to the College network;
- 11.4.2 All images and video of individual pupils or groups of pupils which are delivered to a member of staff as part of their professional work, for example, for an Art display or a marketing initiative, must **not** be stored on any personal computer, the hard drive of any College computer, the memory of any camera or similar device, any personal memory device or other transportable memory and should be uploaded immediately to the College network;
- 11.4.3 Any manipulation or images or video for any purpose including controlled assessment, coursework, marketing, etc., **must** be undertaken on the College network and the results of that manipulation stored on the network only. Exceptionally, Heads of Department may have occasion to transmit

appropriate video and images to the awarding bodies and will be guided in that by the relevant regulations.

12 Data Protection

12.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act - 2018 which states that personal data must be;

- 12.1.1 fairly and lawfully processed;
- 12.1.2 processed for limited purposes;
- 12.1.3 adequate, relevant and not excessive;
- 12.1.4 accurate;
- 12.1.5 kept no longer than necessary;
- 12.1.6 processed in accordance with the data subject's rights;
- 12.1.7 secure;
- 12.1.8 only transferred to others with adequate protection and consent;
- 12.1.9 portable.

12.2 The College will ensure that;

- 12.2.1 it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- 12.2.2 every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- 12.2.3 all personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing';
- 12.2.4 it has a Data Protection policy;
- 12.2.5 it is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
- 12.2.6 Veritau are appointed as the Data Protection Officer;
- 12.2.7 risk assessments are carried out and risk management forms completed as required;
- 12.2.8 it has clear and understood arrangements for the security, storage and transfer of personal data;
- 12.2.9 data subjects have right of access and there are clear procedures for this to be obtained;
- 12.2.10 there are clear and understood policies and routines for the deletion and disposal of data;
- 12.2.11 there is a policy for reporting, logging, managing and recovering from information risk incidents;
- 12.2.12 there are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
- 12.2.13 there are clear policies about the use of cloud storage/cloud computing which ensure that such data transfer/storage meets the requirements laid down by the Information Commissioner's Office;
- 12.2.14 appropriate data protection impact assessments have been conducted.

12.3 Staff must ensure that they;

- 12.3.1 at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- 12.3.2 use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data;
- 12.3.3 transfer data using encryption and secure password protected devices.
- 12.3.4 Are aware of and adhere to the principles set out in Data protection Act 2018.

12.4 The storing of personal data on memory stick or any other removable media should be avoided. In exceptional circumstances, such as an immediate need in relation to a safeguarding incident, this may be necessary. If this is the case staff must ensure that;

- 12.4.1 They have consulted with a senior member of staff;
- 12.4.2 the data must be encrypted, and password protected;
- 12.4.3 the device must be password protected (many memory stick/cards and other mobile devices cannot be password protected);
- 12.4.4 the device must offer approved virus and malware checking software;
- 12.4.5 the data must be securely deleted from the device, in line with College policy once it has been transferred or its use is complete.

13 Communications

13.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the College currently considers the benefit of using these technologies for education outweighs their risks/disadvantages.

	Staff and other adults				Pupils				EYFS	
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted	Permitted	Not Permitted
Mobile phones may be brought to College	✓				✓					✓
Mobile phones used in lessons				✓			✓ e.g. taking a photo of some work for revision purposes			✓

Use of mobile phones in social time	✓					✓ within the mobile phone policy				✓
Staff should only contact a pupil on a College issued mobile device	✓									✓
Taking photographs/film on personal mobile devices or digital camera				✓				✓		✓
Taking photographs/film on College mobile devices or digital camera for College purposes only	✓						✓		✓	
Parent/carer taking photos of a College event on their own device and uploading online with public access				✓				✓		✓
	Staff and other adults				Pupils			EYFS		
Use of personal tablets/laptops/iPads etc. in College				✓				✓		✓
Use of College owned tablets/laptops/iPads in College but not for personal use	✓				✓				✓	
Use of College owned tablets/laptops/iPads out of College but not for personal use	✓ (within the AUP)				✓ (within the AUP)				✓ (within the AUP)	
Only using College provided encrypted storage devices	✓				✓					✓
Use of College e-mail for personal e-mails				✓				✓		✓
Social use of chat rooms/facilities				✓				✓		✓
Use of social network sites in College			✓				✓			✓
Use of educational blogs	✓				✓				✓	

13.2 When using communication technologies, the College considers the following as good practice:

13.2.1 The official College e-mail service may be regarded as safe and secure and is monitored. Staff, Governors, volunteers and pupils should therefore

- use only the College email service to communicate with others when in College or on College systems i.e. by remote access).;
 - 13.2.2 Users should be aware that e-mail communications may be monitored;
 - 13.2.3 Users must immediately report, to the nominated person, in accordance with the College policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;
 - 13.2.4 Any digital communication between staff, governors and pupils or parents/guardians (e-mail, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) College systems. Personal e-mail addresses, text messaging or social media must not be used for these communications;
 - 13.2.5 Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies and not to include any unsuitable or abusive material;
 - 13.2.6 Personal information should not be posted on the College website and only official e-mail addresses will be used to identify members of staff and governors.
- 13.3 Pupils in the EYFS setting only have access to safe and educational sites and are not left on their own with IT equipment.

Pupils in the EYFS setting are not permitted to bring their own devices into College.

14 Social Media – Protecting Professional Identity

- 14.1 All schools have a duty of care to provide a safe learning environment for pupils and staff. The College could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the College liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
- 14.2 The College provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the College through;
- 14.2.1 ensuring that personal information is not published;
 - 14.2.2 training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues;
 - 14.2.3 clear reporting guidance, including responsibilities, procedures and sanctions;
 - 14.2.4 risk assessment, including legal risk.
- 14.3 College staff should ensure that;
- 14.3.1 no reference should be made in social media to pupils, parents/guardians or College staff;
 - 14.3.2 they do not engage in online discussion on personal matters relating to members of the College community;
 - 14.3.3 personal opinions should not be attributed to the College;

- 14.3.4 security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official College social media accounts are established there should be;

- 14.3.5 a process for approval by senior leaders;
 14.3.6 clear processes for the administration and monitoring of these accounts – involving at least two members of staff;
 14.3.7 a code of behaviour for users of the accounts including systems for reporting and dealing with abuse and misuse.

Understanding of how incidents may be dealt with under College disciplinary procedures.

14.4 The College's use of social media for professional purposes will be checked regularly.

14.5 Personal Use

- 14.5.1 Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the College or impacts on the College, it must be made clear that the member of staff is not communicating on behalf of the College with an appropriate disclaimer. Such personal communications are within the scope of this policy.
 14.5.2 Personal communications which do not refer to or impact upon the College are outside the scope of this policy.
 14.5.3 Where excessive personal use of social media in College is suspected and considered to be interfering with relevant duties, disciplinary action may be taken.

15 Monitoring of Public Social Media

- 15.1 As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the College.
 15.2 The College should effectively respond to social media comments made by others according to a defined policy or process.

16 Unsuitable/Inappropriate Activities

- 16.1 Some internet activity, e.g. accessing child abuse images or disturbing racist material is illegal internet activity, e.g. accessing child abuse images or distributing racist material, is illegal and banned from College and all other technical systems. Other activities e.g. cyber-bullying is prohibited and could lead to criminal prosecution. There are however a range of activities which may be, generally, legal but would be inappropriate in the College context, either because of the age of the users or the nature of those activities.
 16.2 The College believes that the activities referred to in the following section would be inappropriate in a College context and that users, as defined below, should not engage in these activities in College or outside College when using College equipment or systems. The College policy restricts usage as follows.

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Promotion of racial or religious hatred					✓
	Any hate crime – motivated by hostility on the grounds of race, religion, sexual orientation, disability or transgender identity.					✓
	Accessing any extremist materials online e.g. Far Right Extremism				✓	
	Promotion or conduct of illegal acts e.g. under the child protection obscenity, computer misuse and fraud legislation					✓
	Adult material that potentially breaches Obscene Publications Act in the UK					✓
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
	Pornography					✓
	Promotion of any kind of discrimination				✓	
	Threatening behaviour, including promotion of physical violence or mental harm					✓
	Promotion of any kind of extremist activity					✓
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute e.g. discussing College issues on social media				✓	
Using College systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the College					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					✓	
Online gaming (educational)			✓			
Online gaming (non-educational)				✓		
Online gambling					✓	
Online shopping / commerce			✓			
File sharing				✓		

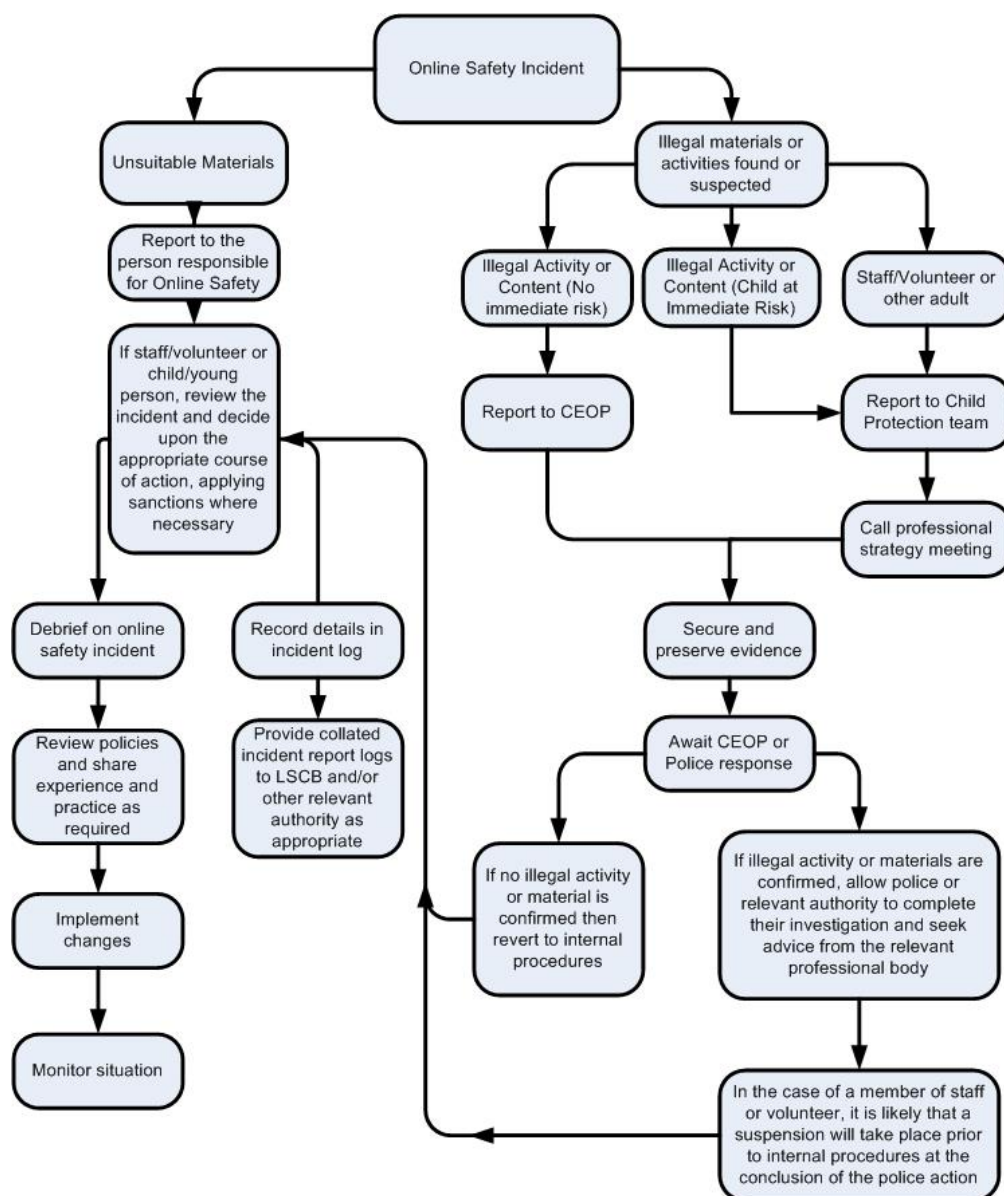
Use of social media		✓			
Use of messaging apps		✓			
Use of video broadcasting e.g. YouTube		✓			

17 Responding to Incident of Misuse

17.1 It is hoped that all members of the College community will be responsible users of digital technologies, who understand and follow College policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

17.2 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the Police.



17.3 If any apparent or actual misuse appears to involve illegal activity the Head will be immediately involved and will report the matter to the Designated Officer (formerly known as the Local Area Designated Officer – LADO) for Child Protection and the Police as appropriate, (as indicated in the Child Protection Policy).

17.4 Other incidents

If members of staff suspect that misuse has taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff will be involved in the investigation which will be carried out on a 'clean' designated computer.

In the event of suspicion, all steps in this procedure should be followed:

- 17.4.1 Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported:
- 17.4.2 Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the Police should the need arise. Use the same computer for the duration of the procedure:
- 17.4.3 It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection):
- 17.4.4 Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below):
- 17.4.5 Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures:
 - Involvement of North Yorkshire Safeguarding Children Board:
 - Police involvement and/or action:
- 17.4.6 If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include;
 - incidents of ‘grooming’ behaviour;
 - the sending of obscene materials to a child;
 - adult material which potentially breached the Obscene Publications Act;
 - criminally racist material;
 - promotion of terrorism or extremism;
 - other criminal conduct, activity or materials.

It is important that all of the above steps are taken as they will provide an evidence trail for the College and possibly the Police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

- 17.5 It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupils**Actions/Sanctions**

Incidents:	Refer to class teacher/form tutor	Refer to Head of Department/Head of Upper or Lower School/ Head of 6th Form/Head of Prep /Head of Pre-Prep or Deputy Head (Pupils)	Refer to Deputy head (Operations/ Online Safety Lead	Refer to Police/External Agency	Refer to IT Manager for action re filtering/security, etc.	Inform parents/guardians	Warning	Removal of network/internet access rights	Further sanction e.g. detention, exclusion
A concern raised by a pupil/teacher/friend/parent (guardian) A pupil needs positive support – Signs of grooming Signs of child on child abuse/grooming/power domination Signs of radicalisation Signs of COE Signs of cyberbullying			✓	✓		✓			
Deliberately accessing or trying to access material that could be considered illegal		✓	✓	✓		✓		✓	✓
Unauthorised use of non-educational sites during lessons		✓					✓		
Unauthorised use of mobile phone/digital camera/other mobile device		✓	✓			✓	✓		✓
Unauthorised use of social media/messaging apps/personal email and online gaming			✓			✓		✓	✓
Unauthorised downloading or uploading of files		✓			✓			✓	
Allowing others to access the College network by sharing user name and passwords		✓						✓	
Attempting to access or accessing the College network, using another pupil's account		✓						✓	
Attempting to access or accessing the College network, using the account of a member of staff			✓			✓		✓	✓
Corrupting or destroying the data of other users			✓			✓		✓	✓
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature			✓	✓		✓		✓	✓

Continued infringements of the above, following previous warnings or sanctions			✓	✓		✓		✓	✓
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College			✓	✓		✓		✓	✓
Using proxy sites or other means to subvert the College's filtering system			✓		✓	✓		✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓				✓		
Deliberately accessing or trying to access offensive or pornographic material			✓		✓	✓		✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓					✓	✓

Staff

Incidents:	Refer to HOD/Line Manager	Refer to Head	Refer to Human Resources	Refer to Police/External Agency	Refer to the ICO	Refer to IT Manager for action re filtering/security, etc.	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal		✓	✓	✓					✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									
Excessive or inappropriate personal use of the internet/social media/personal e-mail	✓					✓			
Unauthorised downloading or uploading of files	✓						✓		
Allowing others to access the College network by sharing user name and passwords or attempting to access or accessing the College network, using another person's account	✓					✓	✓		

Careless use of personal data e.g. holding or transferring data in an insecure manner	✓								
Deliberate actions to breach data protection or network security rules		✓	✓						✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓						✓
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓					✓	✓
Using personal e-mail/social networking/instant messaging/text messaging to carry out digital communications with pupils		✓	✓						✓
Actions which could compromise the staff member's professional standing. In the event of breaches of policy by the Head, refer to the Chair of Governors	✓						✓		
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College		✓					✓		✓
Using proxy sites or other means to subvert the College's filtering system		✓					✓		
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓				✓		
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓				✓	✓
Breaching copyright or licensing regulations	✓								✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓						✓

18 Conclusion

ICT has transformed the ways we communicate with others, both in and out of the classroom. Our aim is to promote the positive use of this technology and to discourage inappropriate usage or usage which could put others at risk. Staff are asked to recognise that this policy is designed above all to protect the interests of the child, to support staff and to ensure that required action is taken as quickly as possible.

Appendix 1

How Will Infringements be Handled?

Whenever a pupil or member of staff infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the College management. The following are set out as guidance based on the level of infringement.

1 Pupils

Category A Infringements

- 1.1 Use of non-educational sites during lessons.
- 1.2 Unauthorised use of e-mail.
- 1.3 Unauthorised use of mobile phone (or other new technologies) in lessons, for example, to send texts to friends.
- 1.4 Use of unauthorised instant messaging/social networking sites.

Possible sanctions

Referred to class teacher or form tutor for a warning and clarification of what can happen if this is repeated/mobile phone removed from pupil and passed to the relevant Deputy Head of Prep School, Head of Lower School, Head of Upper School, Head of Sixth Form or the Deputy Head (Operations) for collection at the end of the College day.

Category B Infringements

- 1.5 Continued use of non-educational sites during lessons after being warned.
- 1.6 Continued unauthorised use of e-mail after being warned.
- 1.7 Continued unauthorised use of mobile phone (or other new technologies) in lessons after being warned.
- 1.8 Continued unauthorised instant messaging/chatrooms/social networking sites.
- 1.9 Use of filesharing software for the purposes of sharing music, games or videos illegally.
- 1.10 Accidentally corrupting or destroying others' data without notifying a member of staff of it.
- 1.11 Accidentally accessing offensive material and/or not notifying a member of staff of it.
- 1.12 Not logging off and/or using another pupils log on details.

Possible Sanctions

Referred to class teacher or Head of Department for follow-up action which could include detention or removal of internet and/or e-mail access for a period of time; mobile phone removed from pupil and passed to the relevant Head of Prep School or the Deputy Head (Operations) who will contact parents regarding collection of the phone and the length of time when the item cannot be brought into College; referred to the Online Safety Lead for a warning of what could happen if this is repeated (particularly for the last two situations).

Category C Infringements

- 1.13 Deliberately corrupting or destroying someone's data, violating the privacy of others.
- 1.14 Sending an e-mail or text message that is regarded as harassment or of a bullying nature (one-off).
- 1.15 Deliberately trying to access offensive or pornographic material.
- 1.16 Any purchasing or ordering of items over the internet (without permission from staff).
- 1.17 Transmission of commercial or advertising material.
- 1.18 Deliberately using another pupil's login details for malicious purposes and/or passing out your personal login details to another pupil.

Possible Sanctions

Referred to relevant Deputy Head of Prep School, Head of Lower School, Head of Upper School, Head of Sixth Form or the Deputy Head (Operations) for a warning and clarification of what can happen if this is repeated and contact with parents as well as removal of internet and/or e-mail privileges for a period of time; referred to the Online Safety Lead for a warning of what could happen if this is repeated (particularly for the last two situations); removal of technological device and parent contacted if this is not done via the College network.

If inappropriate web material is accessed, then ensure the IT Manager is informed and that appropriate technical support filters the site and inform the Deputy Head (Pupils).

Category D Infringements

- 1.19 Continued sending of e-mails or text messages regarded as harassment or of a bullying nature after being warned.
- 1.20 Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- 1.21 Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act.
- 1.22 Bringing the College name into disrepute.
- 1.23 Using the College network as a means of inciting riot or public order offences.
- 1.24 Deliberately trying to circumvent the IT Security Policy.

Possible Sanctions

Referred to Head of Prep School, Deputy Head (Operations), Head, contact with parents which may include exclusion as well as referral to the Community Police; removal of technological device and parent contacted if this is not done via the College network; contact with the Child Exploitation and Online Protection Unit.

If appropriate, secure and preserve any evidence, for example, print-outs of e-mails/texts and inform the sender's service provider.

2 Members of Staff

Category A Infringements (Misconduct)

- 2.1 Excessive use of Internet for personal activities not related to professional development, for example, online shopping, personal e-mail, instant messaging, etc.
- 2.2 Use of personal data storage media (for example, USB memory sticks) without considering access and appropriateness of any files stored.
- 2.3 Not implementing appropriate safeguarding procedures.
- 2.4 Any behaviour on the world wide web that compromises the staff member's professional standing in the College and community.
- 2.5 Misuse of first level data security, for example, wrongful use of passwords.
- 2.6 Breaching copyright or licence, for example, installing unlicensed software on the network.

Possible Sanctions

Referred to Line Manager/Head and warning given.

Category B Infringements (Gross Misconduct)

- 2.7 Serious misuse of, or deliberate damage to, any College computer hardware or software.
- 2.8 Any deliberate attempt to breach data protection or computer security rules.
- 2.9 Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- 2.10 Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act.
- 2.11 Bringing the College into disrepute.

Possible Sanctions

Referred to Head/Governors and follow the College's disciplinary procedures; report to Human Resources/involvement of the Police, if appropriate.

If there is a safeguarding issue, then remove the PC/laptop to a secure place to ensure that there is no further access to the PC or laptop. If appropriate, instigate an audit of all ICT equipment by an outside agency to ensure there is no risk of pupils accessing inappropriate materials in the College. If appropriate, identify the precise details of the materials. In the case of indecent images of children including child pornography being found, the member of staff will be immediately suspended, and the Police should be called. (The College's Child Protection Policy would be implemented.)

Appendix 2 – Useful Resources

The following links may help those who wish further information regarding online safety.

UK Safer Internet Centre

Safer Internet <https://www.saferinternet.org.uk/advice-centre>

South West Grid for Learning - <https://swgfl.org.uk/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Internet Watch Foundation - <https://www.iwf.org.uk/>

CEOP

CEOP - <http://ceop.police.uk/>

Thinkuknow <https://www.thinkuknow.co.uk/>

Others

INSAFE / Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - <http://www.netsmartz.org/>

Bullying/Online-bullying/Sexting/Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyber_bullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children's Commissioner, TES and Schillings – Young peoples' rights on social media](#)

Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

[UKCCIS – Education for a connected world framework](#)

Insafe - [Education Resources](#)

Parents and Guardians

[SWGfL Digital Literacy & Citizenship curriculum](#)

[Online Safety BOOST Presentations - parent's presentation](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops / education](#)

[NSPCC Online Safety <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>](#)

Thinkuknow <https://www.thinkuknow.co.uk/parents/>

Internet mMatters <https://www.internetmatters.org/advice/>

North Yorkshire Safeguarding Children Partnership (NYSCP)

<http://www.safeguardingchildren.co.uk/parents-and-carers>

Safer Internet <http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers>

Appendix 3

Procedure for Managing e-Safe Concerns (Session 2019 – 2020)

The College employs the support of e-Safe in monitoring online safety issues. Concerns are reported to College on a daily basis and a weekly summary is produced. Serious concerns are reported to the College immediately by a telephone call and a subsequent e-mail which is marked with high importance.

Procedure for Following up Concerns

1 Serious Concerns

When serious concerns are reported to the college, the Deputy Head (Operations) or the IT Manager will receive notification and the Deputy Head (Operations) (or in their absence, the DSL) will immediately action any relevant follow-up using the most appropriate member of staff to speak to the pupil.

- 1.1 The allocated member of staff will speak to the pupil and identify whether the concern is justifiably serious and, in discussions with the Deputy Head (Operations) (or the DSL or Deputy DSL's if they are absent), will decide on the appropriate course of action and any subsequent contact with parents/sanctions (if relevant).
- 1.2 Details to be written up using the Online Safety Record of Concern Form.
- 1.3 Any safeguarding issues will be treated appropriately by the DSL or one of the deputies.

2 More Routine Issues

When less urgent issues arise, details of these will be shared with appropriate staff e.g. class teacher, form tutor, Head of Upper or Lower School, to follow up the issues. Generally speaking these will be delegated on receipt of the weekly report.

- 2.1 The allocated member of staff will speak to the pupil and identify whether the concern is justifiable. The member of staff will investigate and decide on the appropriate course of action (if relevant) and if there is no action to be taken, this needs to be agreed with a one of the e-Safety Team members.
- 2.2 If the incident is more serious than anticipated, the member of staff investigating should liaise with either the Deputy Head (Operations) or, in their absence, the DSL.
- 2.3 Details to be written up using the Online Safety Record of Concern Form.
- 2.4 These records will be reviewed at e-Safety Team meetings, in particular to monitor a consistent approach to investigations and actions as well as to look for patterns of concern.

3 Issues Arising During Teaching Lessons

When issues arise during teaching periods (especially relating to curriculum matters), the class teacher may be asked to review the concerns and speak to the individual pupil(s).

- 3.1 The allocated member of staff will speak to the pupil and identify whether the concern is justifiable. The member of staff will investigate and decide on the appropriate course of action (if relevant) and if there is no action to be taken, this needs to be agreed with a one of the e-Safety Team members.
- 3.2 If the incident is more serious than anticipated, the member of staff investigating should liaise with either the Deputy Head (Operations) or, in their absence, the DSL.
- 3.3 Details to be written up using the Online Safety Record of Concern Form.
- 3.4 These records will be reviewed at e-Safety Team meetings, in particular to monitor a consistent approach to investigations and actions as well as to look for patterns of concern.

4 Concerns Involving Members of Staff

When issues arise involving a member of teaching staff, the Deputy Head (Operations) or the DSL will manage the investigation (in consultation with the relevant Line Manager, if appropriate) where that concern is of a serious nature. When issues arise involving a member of support staff, the IT Manager or the Bursar will manage the investigation.

- 4.1 The allocated member of staff will speak to the member of staff and identify whether the concern is justifiable. The member of staff will investigate and decide on the appropriate course of action (if relevant) and if there is no action to be taken, this needs to be agreed with a one of the e-Safety Team members.
- 4.2 If the incident is more serious than anticipated, the member of staff investigating should liaise with the Deputy Head (Operations) or, in their absence, the DSL.
- 4.3 Details to be written up using the Online Safety Record of Concern Form for Staff.
- 4.4 These records will be reviewed at e-Safety Team meetings, in particular to monitor a consistent approach to investigations and actions as well as to look for patterns of concern.

Online Safety Record of Concern

This form should be used to raise online safety concerns about a pupil or member of staff. It should be used to record non-child protection issue like misuse of the College network or mobile devices. When completed this form should be handed to the Head of Upper or Lower School or Deputy Head (Operations) for a pupil and to the Online Safety Coordinator for a member of staff.

Name of Pupil / Member of Staff			
Date of concern being raised		Time / Period	
Online Safety Concern Please record details of the concern / incident	Type of Incident (please tick)		Any Further Details
	☐	Indecent Images	
	☐	Video / music streaming	
	☐	Inappropriate Web searches	
	☐	Social Media Issue	
	☐	Sharing Passwords	
	☐	Other	
Details of Investigation (if relevant)			
Subsequent Actions / Sanctions			
Reasons for <u>no</u> action being taken (if applicable) A 'no action' decision must be agreed and signed by two people			
	Agreed By		Agreed By
Name (Print)			Date
Role			Signature

A copy of this document should be passed to the Deputy Head (Operations) and the IT Manager for filing in the Incident Log.