BLESSED THOMAS HOLFORD
CATHOLIC COLLEGE
Inspiring People – Changing Lives

Online Safety, ICT and internet acceptable use policy

Approved by:	Pupil Welfare and Discipline Committee	**Date:** 03.06.2021
Last reviewed on:	May 2021	
Next review due by:	May 2022	

ICT and Acceptable Internet Use Contents

Online Safety Contents

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers, and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents, and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use
- This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under the following policies:

Pupil Policies

- Behaviour & Learning Policy
- Exclusions Policy

Staff

- Staff Code of Conduct
- Staff Disciplinary Procedure

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2020
- Searching, screening and confiscation: advice for schools

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Executive Headteacher, Head of School or any other relevant member of the Pastoral Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies which are located on our website and for staff the school network (Y:\Staff\School Information\Policies). Sanctions will be dependent on the seriousness of the matter.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The School's IT Network Manager, Data Protection Officer and Named Designated Safeguarding Lead (Associate Headteacher) manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. Staff must ensure these are kept private unless deemed appropriate to share e.g. with the ICT Technicians should there be a fault with their device.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Staff must ensure that all emails are kept professional.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Manager and IT Network Manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils unless there is a compelling reason to do so – e.g. a matter of safeguarding. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided for school trips with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

All recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher and IT Network Manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is always appropriate and professional.

The school has guidelines for staff on appropriate security settings for Social Media accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

For remote access the school use Microsoft's Remote Desktop Services. This is managed in house by the IT Network Manager. Each user needs to log into the Remote Desktop by using their credentials that they use to access the system in school. This will then give the user the right levels of access when using the system.

The link can be found on the Staff shared area if a technician has not already put the link on the user's desktop when their laptop has been setup.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the IT Network Manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.4 School social media accounts

The school has an official Facebook/Twitter/Instagram page, managed by our Marketing Manager and Head of School. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school also have various other Social Media pages relevant to subject areas/extra-curricular, managed by appropriate staff. Staff members who have not been authorised to manage, or post to, on these account, must not access, or attempt to access the account.

The school has guidelines (appendix 5) for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they always abide by these guidelines.

5.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The school monitors ICT use to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures, and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Access to ICT facilities

The school's ICT facilities are available for use by all pupils during timetable lessons and supervised after school activity. The facilities must not be used outside these activities.
Pupils must not use the pc's unless a member of staff is in the room. Sixth Formers are able to use the pc's unattended which are based in the Study Centre. There are also laptops/chromebooks provided to pupils who require them (injury – not able to write etc.), the pupil is required to drop this off with the IT Technician or Head of House.

Pupils may use the following sites to use for subjects, this is not an exhaustive list:

- Kerboodle.com
- Senecalearning.com
- Hegartymaths.com
- Vle.Mathswatch.co.uk
- Google Suite
- Microsoft Teams
- The Edge

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images, anything relating to peer-on-peer abuse, or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet inside and outside of school

The school will sanction pupils, in line with the Behaviour and Exclusion Policies if a pupil engages in any of the following at any time this includes during remote learning (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures or code of conduct
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headteacher's discretion.

Governors may use the ICT facilities for training for their role.

Where Governors and parents are granted access in this way, they must abide by this policy as it applies to staff.

Parent's are asked to read and agree and uphold this policy when their child first enrols with the school and are annually sent the policy for their attention.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

8. Data security

The school takes steps to protect the security of its computing resources, data, and user accounts. However, the school cannot guarantee security. Staff, pupils, parents, and others who use the school's ICT facilities should always use safe computing practices.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure unless deemed appropriate to share e.g. with an ICT Technician to resolve any issues.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way and have a secure access code which is provided by the IT Network Manager.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files, and devices.

These access rights are managed by IT Network Manager.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

Pupils are unable to use external devices to avoid any unnecessary viruses

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT Network Manager.

9. Internet access

The school wireless internet connection is secured.

The web filtering that is used in school is provided by Virtue Technologies. They use the Sophos UDM which provides the school with the relevant filtering. Pupils and Staff have different profiles on the filtering system due to safeguarding etc.

If a parent or external visitor requires access to the school Internet, they will use the Guest access which use the staff profile but has certain sites blocked from access.

9.1 Pupils

Pupils can access the school network by logging in using their accounts that are provided to them when they join in Year 7 or Year 12. They are on a locked down profile which only provides them to sites that are deemed safe. Staff can request for some sites to be unblocked if they are appropriate for educational use. Again, the filtering system is the Sophos UDM. There is a BYOD access in place but as, yet this is to be used by the pupils. If they do need to access to this in the future, then the same profile will apply from the web filtering.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

10. School Monitoring Software

The school uses the monitoring software Impero to ensure pupils are on appropriate websites, it flags any websites and keywords which are deemed inappropriate/offensive.

All Computing and staff deemed relevant by IT Network Manager and Head of School have access to Impero.

The IT Network Manager does a weekly report on any pupils who Impero have flagged up numerous offenses and sends this to the Pastoral Team.

11. Monitoring and review

The Headteacher, IT Network Manager, Data Protection Manager and Assistant Headteacher monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The Board of Governors is responsible for approving this policy.

11. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer 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
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as 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
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

12. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

13. Roles and responsibilities

13.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see ICT and internet use policy)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

13.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

13.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged using CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

13.4 The IT Network manager

The IT Network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged via the DLS on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

13.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see acceptable ICT and internet use policy), and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

13.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see acceptable ICT and internet use policy)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

13.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see acceptable ICT and internet use policy).

14. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum: National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

15. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

16. Cyber-bullying

16.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

16.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. All staff will discuss cyber-bullying with their classes / tutor groups when covered in pupil briefings and PSHCE drop down days.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

16.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

17. Acceptable use of the internet in school

All pupils are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 3) annually, all parents agree to uphold the policy when their child enrols and are sent the policy annually.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

18. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. Mobile phones should not been seen or heard on school grounds.

If phones are used, seen or heard on school grounds they will be confiscated.

If pupils need to contact home during the school day they can do so at pupil services.

19. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on ICT and Internet acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

20. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

21. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using the schools central recording system CPOMs.

This policy will be reviewed every year by the DSL and DPO. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

22. Monitoring and review

The Headteacher, IT Network Manager, Data Protection Manager and Assistant Headteacher monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The Board of Governors is responsible for approving this policy.

23. Links with other policies

This policy should be read alongside the school's policies on:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code
- Data protection policy
- Complaints procedure
- Esafety
- Staff discipline
- Remote learning

Appendix 1: Social Media check sheet for staff

Anything which is posted on social media is considered to be "content" – this includes text for comments, images, videos audio etc. It is important to consider what you post, even if you have high privacy settings anyone can screenshot and repost.

Don't accept or invite friend requests from any current pupils or ex pupils under the age of 18 on social media

Guidance for school staff on Social Media

- Consider changing your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
- Consider changing your profile picture to something unidentifiable, or if not, ensure that the image is professional
- Check your privacy settings regularly, setting your profile to private is considered best practice
- Be careful about tagging other staff members in images or posts
- Don't use social media sites during school hours, which is not related to work (if you schedule content to be posted please let the Named Designated Safeguarding Lead (Associate Headteacher know)
- Don't share content which can lead to possible bullying, bring the school or members of staff into disrepute, release private and confidential information about the school, staff and pupils.
- Don't share content which demonstrates racist, sexist, homophobic, antisemitic, transphobic and other forms of discrimination, harassment or victimisation
- Don't share content which contains lewd, sexually explicit, threatening, inappropriate or offensive comments, images or video clips.
- Don't share content which is defamatory or knowingly false
- Don't share content which breaches copyright infringements to another company
- Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
- Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
- Staff should not accept parents of pupils on their personal social media accounts unless there is an agreed and valid reason
- No communication with parents should be done via social media but should be done through staff emails or via ParentMail

Recording and addressing Social Media Concerns

Any comments, content or interaction that happens on social media platforms that raise a safeguarding concern must be recorded and reported to the Named Designated Safeguarding Lead (Associate Headteacher) as soon as it has been identified.

You can record the concern by saving or screenshotting the content, if it is a video you can record the screen.

Whenever you record any information make a note of the website address, the date and time.

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos**
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name**
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the Names Designated Safeguarding Lead (Associate Headteacher) or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, report immediately to the Headteacher
- If the perpetrator is a parent or other external adult, a senior member of staff should contact them to address any reasonable concerns or complaints and request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should always contact the police. Please report to senior staff immediately

Appendix 2: Social Media check sheet for pupils

Anything which is posted on social media is considered to be "content" – this includes text for comments, images, videos audio etc. It is important to consider what you post, even if you have high privacy settings anyone can screenshot and repost.

Guidance for pupils and students on Social Media

- Check your privacy settings regularly, setting your profile to private is considered best practice
- Don't use social media sites during school hours
- Don't share content which can lead to possible bullying or bring the school into disrepute
- Don't share content which demonstrates racist, sexist, homophobic, antisemitic, transphobic and other forms of discrimination, harassment, or victimisation
- Don't share content which contains lewd, sexually explicit, threatening, inappropriate or offensive comments, images, or video clips.
- Don't share content which is defamatory or knowingly false
- Don't share content which breaches copyright infringements to another company
- Don't associate yourself with the school on your profile

Recording and addressing Social Media Concerns

Any comments, content or interaction that happens on social media platforms that raise a safeguarding concern must be recorded and reported to a member of the Pastoral staff as soon as it has been identified.

You can record the concern by saving or screenshotting the content, if it is a video you can record the screen.

Whenever you record any information make a note of the website address, the date and time.

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos**
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name**
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network or CEOP and ask them to remove it
- If the perpetrator is a current pupil, report immediately to a member of the Pastoral staff.

Appendix 3: Acceptable use agreement for pupils and students

Acceptable use of the school's ICT facilities and internet: agreement for pupils	
Name of pupil:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	Date:

Appendix 4: Link to google form for staff agreement to upload the Online Safety, ICT and internet acceptable use policy

https://forms.gle/gsn7EY2kZLsRogqB6

Appendix 5: Guidelines on what to post on school social media accounts

What to post

Link your posts to what you're trying to achieve with your Facebook page (like parental engagement or marketing to prospective applicants). Make sure posts also reflect your school's ethos and personality.

Dos	Don'ts
Alerts about change (e.g., changes to procedures, severe weather updates)	Names and photos of individuals (unless they've given consent)
Reminders (e.g., approaching deadlines, events or class activities, or reminders about policies/procedures)	Rude, offensive or unprofessional language or content
Adverts for upcoming events	Messages to specific people
Open day dates	Party-political statements
Good luck/congratulations messages for pupils (for example, before exams or after winning a competition)	Adverts for businesses, unless they're directly related to the school (including businesses run by staff, their family, or friends)
Exam results	Links to staff members' personal accounts
Photos or posts about interesting visitors	
Photos of equipment or facilities	
Information about and photos of school trips or clubs	
Links to newsletters and letters for parents	
Seasonal greetings, or messages about religious festivals	
'Getting to know you' posts profiling members of staff	
Details of grants you've been awarded, and what you plan to do with the funding (thank and tag the awarding organisation to increase visibility of the post)	
Information about fundraising activities with a call-to-action (e.g., request for volunteers or link to a crowdfunding page)	
Adverts for school clubs that use your facilities	
Information about local events or points of interest (e.g., local sites, cultural events, summer schools, or new clubs)	
Help and guidance for parents (e.g., e-safety information or factsheets on topical issues)	
Links to news articles about the school	
Alumni news and achievements	
Job adverts or requests for volunteers	
News about staffing changes	
Surveys or polls	