bdat
Bradford Diocesan Academies Trust

ONLINE SAFETY POLICY

Bradford Diocesan Academies Trust

Reviewed: June 24
Next Review Due: June 25

Table of Contents

1. Trust Policy Statement

Bradford Diocesan Academies Trust (BDAT) regards knowing how to stay safe online as integral to the development and safeguarding of our pupils. We are committed to developing a culture where pupils are aware of the risks they face online and know how to keep themselves safe, but where they can also harness the opportunities within the digital world to enhance their education.

We aim to ensure our schools:

- 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
- Establish clear mechanisms to identify, intervene and escalate any online safety incidents including through the use of filtering and monitoring systems

As part of our focus on diversity and inclusion, BDAT pledges that our policies will seek to promote equality, fairness, and respect for all staff and pupils. Our policies reflect the BDAT values of inclusion, compassion, aspiration, resilience, and excellence. By working closely with a range of stakeholders, such as our school, union, and HR colleagues, we have ensured that BDAT's policies do not unlawfully discriminate against anybody.

This policy should be read in conjunction with our school specific Behaviour Policy, Safeguarding Policy and Anti-Bullying Policy, along with other Trust level policies held on the BDAT website. It will be reviewed annually in order to assess its implementation and effectiveness.

This policy has been implemented following consultation with the recognised trade unions and will be reviewed on an annual basis to reflect changes in local and national guidance.

For the purpose of this policy, the term Trust refers to BDAT. The term school and the term academy are interchangeable. The term pupil and the term student are interchangeable.

2. Introduction and Policy Aims

Information and Communications Technology (ICT) in the 21st Century is seen as an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. New technologies have become integral in today's society, both within schools and outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times and, consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies staff, children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, instant messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile phones with text, video and/or web functionality
- Making/receiving phone calls via their mobile phones
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

This policy recognises the commitment of Christ Church Academy to online safety and acknowledges its part in our overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology.

We know about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.

We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The online safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

Keeping Children Safe In Education 2023 references four areas of risk online within part two, these being:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: 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; 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

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through strong educational provision that we build our 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. This involves all stakeholders.

3. Key Staff

The below table details the staff and governors with specific responsibilities relating to online safety:

Role	Name
Designated Safeguarding Lead (Overall Responsibility for Filtering and Monitoring)	Leanne Grimshaw
Deputy Designated Safeguarding Lead	Carole Nightingale Philippa Foster
Safeguarding Team/Other Named Persons	Katie Bellwood Fran Best Amy Conroy Philippa Foster
Nominated Governor for Safeguarding	John Watts
Curriculum Leads with Relevance to Online Safety	Amy Conroy (Computing Lead) Amy Conroy (PSHE Lead)

4. Online Safety Trends

In our school over the past year, we have particularly noticed the following in terms of types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

- Inappropriate use of social media. Children using sites that are classified with an older age rating. Use of social media to harass and bully other pupils. Younger children playing games that are classified with a much higher age rating.

At Christ Church Academy, we are mindful that the online world is ever-developing and we recognise that we must be vigilant in being aware of and responding to new risks that may harm our pupils.

For example, the increasing prevalence of self-generative artificial intelligence is a growing concern, with pupils potentially having access to tools that generate text and images at home or in school.

These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers, and above all, safety. None of the mainstream tools have end-user safety settings and will easily produce inappropriate material despite the age limits that are in place on them.

We recognise that the continued cost-of-living crisis has meant that many children have spent more time online and, as a result, are potentially exposed to all manner of online harms.

Against this background, the Ofcom '[Children and parents: media use and attitudes report 2023]' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further.

As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood, ignored or bypassed, particularly as it can often be the case that children are more technologically literate than many adults.

This is striking when, according to the above report, 20% of 3–4-year-olds have access to their own mobile phone (let alone shared devices), rising to over 90% by the end of Primary School.

Even 3–6-year-olds are being tricked by predators into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home. The 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60% within 12 months to represent over 60,000 cases found.

In the past year, more and more children and young people used apps such as Snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news.

The Revealing Reality: Anti-Social Media Report 2023 highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons.

At the same time, the Children's Commissioner Report 'A lot of it is actually just abuse' revealed the ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys across the world over the past year.

Other issues that have affected many schools across the local authority and nationally include:

- Increase in the number fights being filmed and shared
- Increase in the cases of self-harm and sexual abuse being coerced with threats of violence
- Increase in the number of fake profiles causing issues including:
    - where the school logo and/or name have been used to share inappropriate content about students
    - spreading of defamatory allegations about staff
    - using these fake profile to bully others (sometimes even pretending to be one student to bully a second student)

5. Role and Responsibilities

In the landscape of the challenges outlined above, it is vital that all stakeholders work together to ensure that our pupils remain safe in the online world. This section outlines the roles and responsibilities of the various stakeholders.

5.1 The Local Governing Body

The governing body has overall responsibility for monitoring this policy, holding the Headteacher to account for its implementation and reviewing its effectiveness.

The governing body will ensure that online safety is a focus of its safeguarding quality assurance activities. In particular, the nominated safeguarding governor, John Watts, will monitor the online safety arrangements through regular meetings with the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Ensure that online safety is a running and interrelated theme while monitoring the whole school approach to safeguarding
- Support the work of Christ Church Academy in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- Have an overview of how the school IT infrastructure provides safe access to the internet through its filtering and monitoring systems and the steps Christ Church Academy takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for Christ Church Academy to implement their online safety strategy

5.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout Christ Church Academy. They will:

- Liaise with the Governors to ensure they are provided with relevant online safety information
- Develop and promote an online safety culture within the school community
- Ensure that all staff receive suitable CPD to enable them to carry out their roles in relation to online safety
- Ensure that all staff, pupils and other users agree to the ICT Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Receive and regularly review online safety incident logs through their line management of the Designated Safeguarding Lead; ensuring that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required

5.3 The Designated Safeguarding Lead (DSL)

The details of Christ Church Academy's DSL and deputies are set out in this policy as well as in the Safeguarding and Child Protection Policy and their 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 Christ Church Academy
- Working with the Headteacher, IT staff and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the Christ Church Academy Safeguarding and Child Protection Policy, including making referrals to external agencies such as Children's Social Care, the Police and the Local Authority Designated Officer as necessary.
- Ensuring that any online safety incidents, including those related to filtering and monitoring, are logged on CPOMS and dealt with appropriately in line with this policy
- Work with IT staff to ensure that filtering and monitoring systems are appropriately setup to prevent both under and over-blocking

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Anti-Bullying Policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and Local Governing Body

5.4 IT Staff

The BDAT Head of Corporate Projects is responsible for managing and overseeing the Trust-wide ICT Managed Service Provision, which includes the following:

- 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 whilst at school, including terrorist and extremist material
- Ensuring that Christ Church Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring Christ Church Academy 's ICT systems on an ongoing basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Support Christ Church Academy in providing a safe technical infrastructure to support teaching and learning
- Ensuring appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information and reviewing these regularly to ensure they are up to date
- Ensuring that provision exists for misuse and malicious attack detection
- Ensuring that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems by administrative staff, including password management
- Ensuring that suitable access arrangements are in place for any external users of Christ Church Academy's ICT equipment
- Ensuring appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

5.5 All Staff and Volunteers

All staff and volunteers at Christ Church Academy are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of Christ Church Academy's ICT systems and the internet, 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 on CPOMS and dealt with appropriately in line with this policy
- Reporting any unblocked websites that could be harmful to the DSL
- Informing the DSL if they are teaching any topics that could lead to an influx of filtering and monitoring alerts

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Christ Church Academy Anti-bullying Policy
- Taking responsibility for ensuring the safety of sensitive school data and information
- Developing and maintaining an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintaining a professional level of conduct in their personal use of technology at all times
- Ensuring that all digital communication with pupils is on a professional level and only through school based systems, NEVER through personal email, text, mobile phone social network or other online medium.
- Embedding online safety messages in learning activities where appropriate
- Supervising pupils carefully when engaged in learning activities involving technology
- Ensuring that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable

5.6 Parents

Christ Church Academy would ask that all of our parents and carers support the aims of this policy by:

- Ensuring their child (where age appropriate) has read, understood and agreed to the terms on acceptable use of Christ Church Academy 's ICT systems and internet
- Helping and supporting the school in promoting online safety with their children
- Discussing online safety concerns with their children, showing an interest in how they are using technology, and encouraging them to behave safely and responsibly when using technology
- Consulting with Christ Church Academy if they have any concerns about their child's use of technology
- Supporting the Christ Church Academy approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

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

UK Safer Internet Centre - What are the Issues?
Childnet International - Hot Topics
Childnet International - Parent Factsheet
Safer Internet Day 2023 Film for Parents and Carers
Online Safety Basics - National Cybersecurity Alliance
Parent Zone - Working Towards a Safer Digital World
TALK Checklist by the Internet Watch Foundation

5.7 Pupils

All pupils at Christ Church Academy are expected to:

- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights and values of other pupils in their use of technology at school and at home

- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff in school
- Discuss online safety issues with family and friends in an open and honest way
- Know, understand and follow school policies on the use of technology to an age appropriate level
- Know, understand and follow school policies regarding bullying to an age appropriate level
- Support the Christ Church Academy approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

5.8 Visitors and Members of the Community

Visitors and members of the community who use Christ Church Academy '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.

If visitors are concerned about the welfare of a pupil for any reason, they should report it to the DSL without delay.

6. Educating Pupils about Online Safety

At Christ Church Academy, pupils will be taught about online safety as part of the curriculum. This will be done through:

- An age appropriate curriculum which has online safety related lessons embedded throughout, but with a planned online safety programme as part of the ICT/Computing and PSHE curriculum
- Celebration and promotion of online safety through collective worship and whole-school activities, including Safer Internet Day each year
- Visits from outside agencies such as the police to support the message of staying safe online.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly, keeping personal information private
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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

7. Raising Awareness with Parents and Carers about Online Safety

Christ Church Academy will raise parents' awareness of internet safety in letters or other communications home, including class do – jo, Facebook and twitter and in information via our website. This policy will also be shared with parents. We will let parents know:

- What systems the school uses to filter and monitor online activity
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL or a member of the safeguarding team.

8. Cyber Bullying

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.

Cyber bullying includes sending abusive or hurtful texts, emails, social media posts, images or videos, deliberately excluding others online, spreading nasty gossip or rumours online and imitating others online or using their log-in.

Cyber bullying can be overt or covert but uses digital technologies, including hardware such as computers and smartphones, and software such as social media, instant messaging, texts, websites and other online platforms. Cyber bullying can happen at any time, can be in public or in private online spaces and so is sometimes only known to the target and the person 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.

Christ Church Academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff are 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.

In relation to a specific incident of cyber-bullying, we will follow the processes set out in the Anti-bullying Policy BDAT Anti Bullying 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.

The Headteacher, and any member of staff authorised to do so by them (such as the DSL, senior leaders and the pastoral team), can carry out a search of a pupil in line with DFE Guidance on Searching and Screening and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or;
- Is identified in the school rules as a banned item for which a search can be carried out, and/or;
- Is evidence in relation to a criminal offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or Designated Safeguarding Lead.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated 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 Headteacher, Designated Safeguarding Lead or another member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the Police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or;
- The pupil and/or the parent refuses to delete the material themselves.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on Screening, Searching and Confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

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

9. Acceptable Use of the Internet in School

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Christ Church Academy 's ICT systems and the internet. Visitors will also be expected to read and agree to Christ Church Academy's terms on acceptable use if relevant.

Use of Christ Church Academy'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) through our filtering and monitoring systems to ensure they comply with the BDAT Acceptable Use of IT Policy.

10. Pupils Using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them whilst on school site unless given specific permission by a member of staff. They should be switched off and given to the office before entering school. They should be collected at the office at the end of the school day.

11. Staff Using School Devices Outside Work

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

BDAT ensures that all laptops provided for use inside and outside school have:

- Anti-virus and anti-spyware software installed
- Up-to-date operating systems with the latest updates installed

Staff members must not use the device in any way which would violate the BDAT Acceptable Use of IT Policy. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from a member of IT support.

12. Responding to Issues of Misuse

Where a pupil misuses Christ Church Academy's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 Christ Church Academy'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 disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Christ Church Academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the Police.

13. IT Systems and Access

In partnership with our trust-wide IT Managed Service Provision, Christ Church Academy decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their role in school and will be responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Pupils are taught about safe practice in the use of their log in and passwords.

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

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

Our practice in relation to passwords is as follows:

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

- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.
- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- We maintain a log of all accesses by users and of their activities while using the system in order to track any online safety incidents. Class teachers closely monitor the use of the internet by pupils in school.
- Passwords must be difficult to guess and should be a mixture of upper case and lowercase, numbers and symbols.
- Staff and pupils will have to reset their passwords at given intervals.

14. Filtering and Monitoring

14.1 Filtering

In order to ensure that appropriate online filtering is in place across our network, Christ Church Academy use Securly, a cloud-based web filter which is designed specifically for schools. Securly blocks internet access to harmful sites and inappropriate content, meeting all of the technical requirements set out by the Department for Education and specifically blocking access to illegal content including child sexual abuse material.

The Securly filtering system filters all internet feeds, across all devices and operating systems, providing visibility into online activity by alerts to the DSL when there are attempts to access any web content that has been blocked.

Securly identifies the device/IP address (and where possible the individual), time and date of attempted access and the search term or content being blocked. Securly is customisable to ensure the provision meets the ongoing needs of Christ Church Academy, our pupils and our staff.

We have support via a managed IT service desk whose staff are trained on the Securly system and can make real-time changes should a site need to be blocked/un-blocked urgently.

As an additional check, the DSL checks that our internet filtering is effective in blocking certain harmful material by using http://testfiltering.com/

Securly have been members of the Internet Watch Foundation since 1st March 2016.

14.2 Monitoring

As an additional safeguard Christ Church Academy have keystroke monitoring in place through Smoothwall Monitor, who have been a member of the Internet Watch Foundation since 1st June 2007.

Smoothwall Monitor is a real-time, digital monitoring solution that flags safeguarding incidents as they happen when users view or type harmful content. This is able to capture activity that may indicate a risk, even outside of the regular web browser – such as in a Microsoft Word document etc.

All Smoothwall Monitor alerts are reported to the DSL via an email alert so that a safeguarding response can be implemented. Where there is an immediate risk of harm, Smoothwall Monitor will phone the school immediately.

15. Using the Internet and Email

We provide the internet to:

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

Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

All email activity is recorded in line with data protection laws. The school is able to view these records in situations where this is called upon.

Christ Church Academy will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils. Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses.

16. Publishing Content Online

Christ Church Academy maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. We maintain the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number.

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

Material published by pupils, governors and staff in a social context which is considered to bring Christ Church Academy into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

We recognize that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished.

Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Identities of pupils are protected at all times and, in line with GDPR regulations, parents have the option to opt out so that photographs of individual pupils are not published on the website without permission. Group photographs do not have a name list attached.

For their own protection, staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events, except in specific circumstances where rights holders refuse permission, but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites and can be only used for their personal use.

17. 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 other children online through:
    - Abusive, harassing, and discriminatory 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 safeguarding team 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.

18. Policy Monitoring Arrangements

This policy will be reviewed every year by the Headteacher and ratified by the Local Governing Body. Given the ever-changing nature of technology, we will ensure that this review is supported by ongoing risk assessment which reflects current online safety issues that children face. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

We will monitor the impact of the policy using:

- Logs of reported incidents in the Online Safety and Filtering and Monitoring categories on CPOMS
- Internal monitoring data for network activity gathered through filtering and monitoring software
- Pupil, staff and parent voice

19. Links to Other Guidance and Policies

This policy reflects existing legislation, including but not limited to The Malicious Communications Act 1988, 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 takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

It should also be read in conjunction with the following guidance and other BDAT/Academy specific policies:

- Keeping Children Safe in Education 2023
- Relationships Education, Relationships and Sex Education and Health Education - September 2021
- Teaching Online Safety in Schools - January 2023
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation
- Protecting children from radicalisation
- Sharing Nudes and Semi-Nudes Advice for Education Settings - December 2020
- Guidance for Safer Working Practice in Education Settings - February 2022
- DFE Digital and Technology Standards - March 2023

- NPCC Guidance for Schools on When to Call the Police

- BDAT Equality Statement and Objectives
- BDAT GDPR Policy
- BDAT Acceptable Use of IT Policy
- BDAT Social Media Policy

- CCA Behaviour policy
- CCA Child Protection & Safeguarding policy