Bury Catholic Preparatory School

Computing and Online Safety Policy

Created by: ICT Coordinator
Ratified by Governors
Reviewed: July 2020
To be reviewed: July 2021

Computing and Online Safety Policy

Mission Statement

BCPS is a happy and caring school community.
We follow Jesus' example to respect, value and nurture every unique individual to develop their God given talents and potential.
We are a school where faith and future flourish.

Introduction

This policy sets out Bury Catholic Preparatory School's aims and strategies for the successful delivery of Computing. This policy should be read in conjunction with other relevant school policies such as the Safeguarding, Equal Opportunities, Curriculum, Finance, Teaching & Learning, SEND and Assessment policies.
The policy has been developed by the Computing Leader (Helen Lent) in consultation with the SENCO, Leadership Team and teachers. Guidance from consultants and pupil, parent and staff voice have shaped and will continue to help shape this policy. This policy is based on government recommended/statutory programmes of study.

Due to the fast pace of technology innovation and constantly emerging trends, it is recommended that this policy is reviewed, at minimum, at the start of every academic cycle.

Aims

Bury Catholic Preparatory School believes that every child should have the right to a curriculum that champions excellence; supporting pupils in achieving to the very best of their abilities. We understand the immense value technology plays not only in supporting the Computing and whole school curriculum but overall in the day-to-day life of our school.
We believe that technology can provide: enhanced collaborative learning opportunities; better engagement of pupils; easier access to rich content; support conceptual understanding of new concepts and can support the needs of all our pupils.

We aim to:

- Provide an exciting, rich, relevant and challenging Computing curriculum for all pupils.
- Enthuse and equip children with the capability to use technology throughout their lives.
- Give children the access to a variety of high-quality hardware, software and unplugged resources.
- Instil critical thinking, reflective learning and a 'can do' attitude for all of our pupils, particularly when engaging with technology and its associated resources.
- Teach pupils to become responsible, respectful and competent users of data, information and communication technology.
- Teach pupils to understand the importance of governance and legislation regarding how information is used, stored, created, retrieved, shared and manipulated.
- Equip pupils with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimise the risk to themselves or others.
- Use technology imaginatively and creatively to inspire and engage all pupils, as well as using it to be more efficient in the tasks associated with running an effective school.
- Provide technology solutions for forging better home and school links.
- Utilise computational thinking beyond the Computing curriculum.
- Exceed the minimum government recommended/statutory guidance for programmes of study for Computing and other related legislative guidance (online safety).

Safeguarding: Online Safety

Online safety has a high profile at Bury Catholic Preparatory School for all stakeholders. We ensure this profile is maintained and that pupil needs are met by the following:

- A relevant up-to-date online safety curriculum which is progressive from Early Years to the end of Year 6.
- A curriculum that is threaded throughout other curriculum areas and embedded in the day-to-day lives of our pupils.
- Training for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- Throughout home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.
- Pupils, staff and parents have Acceptable Use Policies which are signed, and copies freely available.
- Our online safety policy (part of our Computing policy) clearly states how monitoring of online safety is undertaken and any incidents/infringements to it are dealt with.

- Filtering and monitoring systems for all of our online access.
- Data policies which stipulate how we keep confidential information secure.

Curriculum

As a school, we have chosen the Espresso and Purple Mash Computing Schemes of Work from Reception to Year 6. The schemes of work support our teachers in delivering fun and engaging lessons which help to raise standards and allow all pupils to achieve to their full potential. We are confident that the schemes of work more than adequately meets the national vision for Computing. It provides immense flexibility, strong cross-curricular links. Furthermore, it gives excellent supporting material for less confident teachers.

Early Years

We aim to provide our pupils with a broad, play-based experience of Computing in a range of contexts. We believe the following:

- Early Years learning environments should feature Computing scenarios based on experience in the real world, such as in roleplay.
- Pupils gain confidence, control and language skills through opportunities to 'paint' on the interactive board/devices or control remotely operated toys.
- Outdoor exploration is an important aspect, supported by Computing toys such as metal detectors, controllable traffic lights and walkie-talkie sets.
- Recording devices can support children to develop their communication skills. This is especially useful for children who have English as an additional language.

Key Stage 1 outcomes

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions.
- Write and test simple programs.
- Organise, store, manipulate and retrieve data in a range of digital formats.
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

Key Stage 2 outcomes

- Design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- Use sequence, selection and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs.
- Use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs.
- Understand computer networks including the internet; how they can provide multiple services, such as the world- wide web; and the opportunities they offer for communication and collaboration.
- Describe how Internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Assessment

Pupil attainment is assessed using the 2Simple Computing Assessment Tool for Years 1 to 6. The tool enables staff to accurately identify attainment of pupils through the detailed exemplification it has for each key learning intention.

- A relevant up-to-date Online safety curriculum which is progressive from Early Years to the end of Year 6.
- A curriculum that is threaded throughout other curriculums and embedded in the day-to-day lives of our pupils.
- Training for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- Through our home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.
- Pupils, staff and parents have Acceptable Use Policies which are signed and copies freely available.
- Our Online Safety Policy (part of our Computing policy) clearly states how monitoring of online safety is undertaken and any incidents/infringements to it are dealt with.
- Filtering and monitoring systems for all our online access.

- Teachers keep accurate records of pupil attainment by entering data using the 2Simple Computing Assessment Tool.
- Tracking of attainment by using the 2Simple Computing Assessment Tool is used to inform future planning.
- Children are encouraged to self, peer and group assess work in a positive way using online collaborative tools such as 2Blog.
- Formative assessment is undertaken each session/interaction in Computing and pupils are very much encouraged to be involved in that process. Through using the progression of skills documents and displays from 2Simple, both teachers and pupils can evaluate progress. Features such as preview and correct in Purple Mash are used to further support feedback and assessment.
- Summative assessment is undertaken in line with the assessment cycle (See Assessment Policy). Using electronic work samples from children's portfolios on Purple Mash, teachers enter judgements about the samples into the 2Simple Computing Assessment Tool.
- Work from a range of classes and abilities is shared using the Noticeboard feature in Purple Mash.

Resources

- All resources are procured with the underlining considerations of value: The extent at which the resource impacts on learning and the material cost of this. Protocol details for procurement can be found in the school finance policy.
- A range of resources is available which successfully supports delivering the Computing curriculum and enables all learners to reach their full potential.
- Resources are suitably maintained and replenished when needed, which is overseen by the Computing Leader. An itemised list of all resources is shared with staff and kept up to date by the Computing Leader.
- Audits of school resources are conducted regularly by the Computing Leader.
- The Computing Leader keeps up to date with the latest technology resources and will make informed decisions about possible procurement of them through their own research.
- Suggestions for getting the very best out of the resources are made available to teaching and support staff by the Computing Leader.

Inclusion

At Bury Catholic Preparatory School, we aim to enable all children to achieve to their full potential.

This includes children of all abilities, social and cultural backgrounds, those with disabilities, EAL speakers and SEN statement and non-statemented.
We place particular emphasis on the flexibility technology brings to allowing pupils to access learning opportunities, particularly pupils with SEN and disabilities. With this in mind, we will ensure additional access to technology is provided throughout the school day and in some cases beyond the school day.

Monitoring, Evaluation and Feedback

Monitoring standards of teaching and learning within Computing is the primary responsibility of the Computing Leader. All teachers are expected to ensure that children's work is saved on Purple Mash or on the Shared Drive, and that objectives covered are assessed in the children's Computing Booklets. The online areas must contain work samples from all areas of the curriculum taught for the year group.

Monitoring will be achieved through:

- Work scrutiny.
- Learning walks.
- Observations.
- Pupil voice.
- Teacher voice.
- Reflective teacher feedback.
- Learning environment monitoring.
- Dedicated Computing Leader and Assessment Leader time.

Evaluation and Feedback will be achieved through

- Using recognised standards documentation for end-of-year expectations.
- Using recognised national standards for benchmarking Computing provision in primary schools.
- Written feedback on evaluation of monitoring activities to be provided by the Computing Leader in a timely manner.
- Feedback on whole school areas of development in regard to Computing to be fed back through insets/AOB/staff meetings.

Roles and Responsibilities

Due to technology extending beyond the National Curriculum for Computing, there are key roles and responsibilities specific
members of staff have.

Headteacher:

- Monitoring the implementation of the Computing Policy and its associated policies such as the Safeguarding and SEND Policies.
- Ratifying (in conjunction with the Governing Body) the Computing policy and Safeguarding policy.
- Securing technical support service contracts and infrastructure maintenance contracts. Approving CPD and training which is in line with the whole school's strategic plan.
- Approving budget bids and setting them.
- Creating in conjunction with the Computing Leader, a long-term vision for Computing which includes forecasted expenditure and resources.
- Monitoring the performance of the Computing Leader in respect to their specific job role description for Computing.
- Ensuring any government legislation is being met.

Computing Leader:

- Raising the profile of Computing for all stakeholders.
- Monitoring the standards of Computing and feeding back to staff in a timely fashion so they can act on areas for development.
- Ensuring assessment systems are in place for Computing.
- Maintaining overall consistency in standards of Computing across the school.
- Reporting on Computing at specific times of the year to the Governing Body/Head/Staff.
- Auditing the needs of the staff in terms of training/CPD. Actively supporting staff with their day-to-day practice.
- Seeking out opportunities to inspire staff in developing their practice through modelling and sharing new ideas, approaches and initiatives.
- Attending training and keeping abreast with the latest educational technology initiatives.
- Using nationally recognised standards to benchmark Computing.
- Creating Action Plans for Computing and supporting a long-term vision which feeds into the whole school development plan.
- Keeping an up-to-date log of all resources available to staff.
- Procuring physical and online resources that demonstrate best value. Reviewing the Computing curriculum and developing it as needed.
- Overseeing the effectiveness of the technician.
- Working as needed with the SENCO/Head Teacher to ensure online safety provision is above adequate and all legislation is in place.

Technician:

- Conducts routine scheduled maintenance/updates on systems.
- Fixes errors/issues with hardware and software set-up, prioritising as needed.
- Routinely checks school filtering, monitoring and virus protection.
- Sets up new hardware and installations.
- Maintains network connectivity and stability.
- Supports the Computing Leader and Head Teacher with future infrastructure needs and associated projected costs.

Administration Staff:

- Maintains the school website content (with support from Computing Coordinator).
- Posts approved requests to the school's social media accounts.
- Supports procurement of resources and technical services.
- Supports the technician with some data management.

Health and Safety

Bury Catholic Preparatory School takes all necessary measures to ensure both staff and pupils are aware of the importance of health and safety.
Both staff and pupils are trained to handle electrical equipment correctly including how to power off and on. Pupils are reminded about the dangers of electricity and the danger signs to look out for. Adequate displays and warning signs are strategically placed around the school to reinforce health and safety.

Online Safety

Introduction

At Bury Catholic Preparatory School we are committed to ensuring that children learn how to use computers, Computing and modern technologies safely so that they:

- Are able to use Computing safely to support their learning in school.
- Know how to use a range of Computing equipment safely.
- Are able to use Computing and modern technologies outside school in a safe manner, including using Computing as a tool for communication.
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner.
- Know what to do if they feel unsafe when it comes to using technology and Computing

This policy outlines the steps the school takes to protect children from harm when using Computing and also how the school proactively encourages children to develop a safe approach to using Computing whether in school or at home.

1. 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and Guidance:

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

3. Roles and Responsibilities

Governors will:

- Ensure that the school is implementing this policy effectively.
- Adhere to the acceptable use agreement when in school.
- Have due regard for the importance of online safety in school.

The Headteacher will:

- Ensure the policy is implemented, communicated and compliance with the policy is monitored.
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 1).
- Ensure that staff understand this policy, and that it is implemented consistently throughout the school.
- Ensure staff training in online safety is provided and updated annually as part of safeguarding training.
- Ensure immediate action is always taken if any risks or dangers are identified, e.g. the reporting of inappropriate websites.
- Ensure that all reported incidents of cyber bullying are investigated.
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material.

Computing Leader will:

The school's Computing Leader will work alongside the school's safeguarding team, staff, headteacher and the IT support team, taking a role in the responsibility of online safety. This includes:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (see appendix 4) 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 3 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.
- Ensuring that any online safety incidents are logged (see appendix 4) 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.

<u>The IT Technician (RS-IT Solutions)</u>
RS-IT Solutions is responsible for:
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's IT 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 IT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that antivirus software has been installed on all computers and is to be maintained and updated regularly.
- Ensuring that electronic items which are used by staff are securely stored and password protected.

This list is not intended to be exhaustive.

<u>All staff and volunteers</u>
All staff, including contractors, students, volunteers and agency staff 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 IT systems and the internet (appendix 2) and ensuring that pupils follow the school's terms on acceptable use (appendix 1).
- Monitor and supervise pupils' internet usage and use of other IT resources.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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
- Keep passwords private and only use their own log in details, which are stored securely.
- Promote online safety and teach e-safety units as part of the computing curriculum.
- Engage in online safety training.
- Only download attachments/material onto the school system if they are from a trusted source.
- When taking pictures/videos/sound clips of children, only use school cameras, iPads and recording device.

This list is not intended to be exhaustive.
It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members and the reputation of the school are safe guarded. In this context, staff members but conscious at all times of the need to keep their personal and professional lives separate.

<u>Parents</u>
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 IT systems and internet (appendix 1).

- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issues
    - Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
    - Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the school's IT 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 (appendix 2).

4. Teaching and Learning

At Bury Catholic Preparatory School, pupils will be taught about online safety as part of the curriculum, at an age appropriate level. We use several sources (Knowsley Scheme, Purple Mash, Espresso, Google Be Responsible) in each year group to cover: what should and shouldn't be shared online, password control and cyber-bullying among other topics. Online safety will also be embedded throughout learning whenever children are using technology in other lessons.

In Key Stage 1, pupils will be taught to:

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

Pupils in Key Stage 2 will be taught to:

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

5. 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.

6. Cyber-bullying

Definition:

The definition of cyber-bullying and other online terms can be found in the glossary in Appendix 5. 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).

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. Class teachers will discuss cyber-bullying with their class and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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.

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Mobile phones for children are not permitted in school. All mobile phones brought into school by pupils are held in the school office until the end of the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device (laptop or iPad) outside school must not install any unauthorised software or apps on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any sensitive data held on devices (e.g. SEN data must be saved as a password protected document). If staff have any concerns over the security of their device, they must seek advice from the RS-IT Solutions. Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse.

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour 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 disciplinary

procedures. 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.

11. 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).

Staff 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.

Appendix 1: Acceptable Use Agreement (pupils and parents)

Acceptable Usage Policy for Parents and Pupils

Mission Statement
BCPS is a happy and caring school community. We follow Jesus' example to respect, value and nurture every unique individual to develop their God given talents and potential. We are a school where faith and future flourish.

Please return signed form to school

Pupils and Parents
Academic year 2020-2021

This is the acceptable usage policy for our school. The purpose of this policy is to promote positive and responsible network and internet behaviour. **Please read carefully and sign at the bottom to show you agree to these terms, and then return to the office.**

For pupils:

• I will only use the school internet and network for my school work or when a teacher has given permission.
• I will only use my school email address when using email in school (if applicable)
• I will be careful when opening emails from people I don't know and I will ask an adult if I'm unsure whether to open it.
• I will not share my internet or network passwords.
• I will not look at or delete other people's work or files.
• I will make sure all my contact with other people at school is responsible. I will not cyber-bully pupils or teachers.
• I won't look for or look at unpleasant or inappropriate web sites. I will check with a teacher if I think a website might be unsuitable.
• I won't give out my personal details, such as my name, address, school or phone number on the internet.
• I understand that meeting people in real life who I first met online is dangerous. If someone is asking to meet me in real life I will inform my parents or carers immediately. I will not arrange to meet them by myself.
• I won't upload or download any pictures, writing or movies which might upset people or make other people think the school is a bad place.
• I won't try to install software onto the school network because it might have a virus on and cause a lot of damage. Instead I will ask a teacher for advice.
• I will be careful with keyboards, mice, headphones and all other equipment, and when turning a computer on or off.
• I know that everything I do on the computers at school is recorded and that the school can talk to my parents if a teacher is worried about my online safety.
• I will try to follow these rules all the time because I know they are designed to keep me safe.
• Images of pupils will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the internet, in the press, or in media**,** with permission from the Headteacher.

Signed: - Pupil: _____

Print Name_____

For parents:

• I agree to support and uphold the principles of this policy in relation to my child and their use of the internet, at home and at school
• I agree to uphold the principles of this policy in relation to my own use of the internet, when that use is related to the school, employees of the school and other students at the school.
• I will be aware and circumspect about sharing my own contact details or information and will not share that of others without their permission.

Signed:-Parent/Guardian:_____

Date: _____Print Name _____

Appendix 2: Acceptable use agreement (staff)

Bury Catholic Preparatory School
Social Networking and Acceptable Use
Mission Statement

BCPS is a happy and caring school community.
We follow Jesus' example to respect, value and nurture
every unique individual to develop their God given talents and potential.
We are a school *where faith and future flourish*.

This policy and its content is effective immediately. The purpose of this policy is to protect staff, children and the school's reputation. No school equipment should be used for personal use- whether this is for social networking or personal emails or printing etc Any staff using social networking sites e.g. Facebook/Twitter should only do so in their own time (breaks, lunches) and in an area where parents/children are not likely to see (staff room etc).

Procedures

- Staff may not be Facebook friends with parents they have no personal links with ie they are just parents of children in their class etc, Parents will be advised of this, and this must be put in place immediately
- Staff can be Facebook friends with colleagues.
- Where staff have another relationship with some parents- children in same class who are friends for example- they can be friends on Facebook but must be circumspect, check their privacy settings and ensure that comments are not related to work.
- Staff should not be friends with present or past pupils under the age of 16.
- Staff must not make reference to the school, its customers or its staff on social networking sites. It is strongly recommended that you do not include your place of work in your profile
- Staff should only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of the head teacher.
- Staff should not divulge any school related passwords and they should comply with school IT security procedures.
- Staff should make sure email and social media interactions with staff, parents, pupils and members of the public are responsible and in line with school policies and DfE guidelines.
- Staff should not give their home address, phone number, mobile number, personal social networking details or email address to pupils. School accept that pupils may find these details out, and that any contact should be logged and either not reciprocated, or replied to in line with school policies. Staff should be responsible and aware of their professional responsibilities and school policies if they supply any personal details to parents.
- Staff should use school email systems for school related communications. Staff should not use personal accounts for school business.
- Staff should ensure that personal data is stored securely and in line with the General Data Protection Regulations. Staff should follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment.
- Staff should not install software onto workstations or the network unless supervised by the Network Manager or IT support staff.
- Staff should not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory or copyright infringing.
- Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written permission has been granted by the subject of the photograph or their parent/guardian. Staff should ask the permission of the Head teacher prior to taking any photographs.
- Staff are aware that all network and internet activity is logged and monitored and that the logs are available to the Head teacher in the event of allegations of misconduct.
- Staff should not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in any way which might bring the school into disrepute.

- Staff should make sure that their internet presence does not bring the teaching profession into disrepute and that they behave online in line with DfE and GDPR guidelines.
- Staff should support and promote the school's e-Safety policy and be a role model for positive and responsible behaviour on the school network and internet.

Privacy

- To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly and we recommend the following:
- **Privacy Setting Recommended security level**
  All settings should be 'friends only

Signed: _____

Date:_____

Breaches of this policy may result in disciplinary action being taken.

Appendix 3: Online Safety Training Needs – staff self-audit

Online Safety Training Needs Audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's IT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: Online Safety Incident Report Log

Online Safety Incident Report Log

Date	Where did the incident take place?	Describe the incident	Action Taken	Name and signature of staff member recording the incident.

Appendix 5: Glossary of Online Safety Terms (staff use)

Terminology	Meaning
Ardware	Software application which displays adverts and can redirect searches.
App	Short for application, typically used to refer to a piece of software designed for a particular purpose.
Block	To block someone from contacting a user on a social media account for example.
Blog/Blogging	An updated webpage containing users' opinions/experiences/ observations.
Bot	A program that can do things without a user needing to give instructions. Many bots are malware.
CEOP	Child Exploitation and Online Protection Command is tasked to bring offenders to UK Courts.
Chatroom	A place on the internet where one or more people can chat.
Chatroulette	Strangers interacting over text-chat and webcam. Lots of users post sexual images.
Circumventor Sites	Parallel websites that allow children to bypass sites their adults have blocked.
Cookie	A small file which records a user's personal preferences, shopping choices and other information.
Creeping	Someone who follows someone else's social network profile closely.
Cyberbullying	The use of electronic communication to bully someone.
Decoy App	These apps help children hide videos/images from their parents.
Digital Footprint	A person's trail of data on the internet that can last indefinitely.
Emoji	A small digital image used to express an idea, action or emotion in electronic communication.
Fabotage	Accessing someone else's social media account without their knowledge and changing information on it.
Firewall	A security system that protects an internal network from an external one such as the internet.
Gamer	A person who plays video games including online, likely with other online users.
Gamer Tag	An alter ego made from an alias, picture or avatar. Sometimes these are offensive.
Griefer	Someone who deliberately harasses online gamers during a gaming session.
Grooming	Someone who gains a child's trust for sexual exploitation or trafficking.
Hacker	A person who uses technology to gain unauthorised access to information.
Identity Theft	A crime where data is pieced together from an individual to impersonate them for financial gain.
IM	Instant message sent between users via the internet. These are very popular with younger generations.
In-app purchasing	Purchases of services or products are possible within some apps, such as game apps, and real money is required by them.
Incognito browsing	This allows a user to browse the web without their history being recorded on their device.
ISP	An internet service provider gives access to the internet. ISPs have to comply with the Investigatory Powers Act 2016.
Malware	Software which is made to disrupt, damage or gain unauthorised access to a device.
Netiquette	Netiquette is the code of good behaviour on the internet. As the internet changes, so does netiquette.
Pharming	Directing a user to a bogus website that pretends to be a real one in order to extract information from them.
Phishing	Emails which appear legitimate but are fake, and entice a recipient to share confidential information.
Photo Sharing	Some apps allow users to share images for a few seconds. These apps can be very damaging to children.
PM (or DM)	Private or personal (or Direct) message sent via the internet. Popular feature available on many social media platforms.
Profile	Often social media sites will allow users to create their own personal profiles which other users can see.
Selfie	Self-portrait photo often taken at arm's length using a Smartphone and uploaded to social media.
Sexting	Sending and receiving sexually explicit images/videos via IM, text or social media.

Social Media	Websites and applications where users can share content and participate in social networking.
Spam	Messages sent to large numbers of users for the purpose of phishing, spreading malware and advertising.
Spyware	Software that covertly collects information from a device without the device user's permission.
Trojan	A type of malware which is disguised as legitimate software and accesses confidential information.
Troll	A user who posts inflammatory messages typically on Social Media sites to upset others.
Video Hosting Sites	Websites and apps which allow users to post and view video clips, like YouTube.
Virus	A virus can do many things such as steal data and control a device. They are often caught from email attachments and downloading from a website.