Barndale House School

What I learn today, prepares me for tomorrow.

Digital Safety Policy 2022-2023

Policy Location:	Written:	Review Due:	Person Responsible:
Staff Share -> Policy Library	January 2022	January 2023	Mark Phillips Helen Hemsley

Contents

1. Aims

Barndale House School works with a broad range of learners with complex needs. Many of our students have access to the digital world through a variety of devices within school and at home. We recognise both the value and the vulnerabilities this brings and as such will capture these in this policy along with appropriate measures to safeguard our young people. This policy will also share how we support parents, carers and families in ensuring they can sufficiently safeguard their children at home.

This policy will also ensure staff have a clear understanding of how they can keep themselves safe online and signpost them to training, support and guidance.

Barndale House School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors when using digital devices
- Deliver an effective approach to online safety, which supports 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
- Develop confidence in becoming a positive digital citizen, including how to manage digital footprints and vulnerability online.

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

2. 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 head-teachers 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.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the head-teacher to account for its implementation.

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

The governor who oversees online safety is Mrs Hannah Moeini.

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.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted as necessary for SEND pupils , vulnerable children and victims of abuse 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

3.2 The SLT

The SLT will:

- Ensure that staff have read and understood this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL)

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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with ICT support 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 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 agreed policy and procedure
- Updating and delivering staff training on online Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the governing board

This list is not intended to be exhaustive.

3.4 Infrastructure Support

Northumberland County Council are 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 regular basis.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring the software network and hardware needs fall in-line with GDPR and data protection requirements.

This list is not intended to be exhaustive.

3.5 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 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
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the agreed school policy and procedures
- 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.

3.6 Parents and Carers

Parents are expected to:

- Notify a member of staff or the head teacher of any concerns or queries regarding this policy
- Ensure, as far as is possible ,that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

3.7 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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the Computing and PSHE (including RSE) curriculum.

Pupils will be taught:

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

As Barndale House is an all age specialist school students will follow a phased curriculum. This is to ensure any previous gaps in learning are covered but also to match the curriculum to their social, emotional and developmental needs.

Engage	Activate				Consolidate
Class 1	**Class 2**	**Class 3**	**Class 4**	**Class 5**	**Class 6**
Staying safe – following SMART rules when online Making safe choices Introduction to passwords Seeking permission Following (safe) routines	Online Safety and digital literacy skills(1)(2) Using the Internet - safe searching E-mailing – safe communication skills Personal and private information Digital footprints Exploring websites safely Online behaviour Identifying possible dangers online.	Online Safety and digital literacy skills (3) (4) Introduction to cyber-bullying Reporting concerns Online advertising Developing strong passwords Sending and receiving emails safely Online communities Digital citizenship	Online Safety and digital literacty skills (5) (6) Identify spam emails Create a strong password using a set of rules Analysing online information Identify unsafe behaviour online Recognising impact of false advertising /fake news Stereotypes Online security	Online Safety and digital literacy skills (7) (8) Networking Saving work securely Understanding how to report concerns Communicating online safely and respectfully Assess the quality and validity of digital resources/information Creating and sharing content Social Media	Safe use of technology in everyday tasks Digital resilience My online reputation Long term consequences of irresponsible actions Online relationships Online grooming Adult content Being a critical consumer Recognising bias, propaganda and manipulation

Expectations

When they leave Barndale House School pupils will know:

- A range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- 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
- 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
- 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

- 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 content of online safety sessions will often be taught as part of the Computing and PSHE programme of study however the safe use of social media and the internet will also be covered in other subjects where relevant. It is likely that sessions will be tailored to fit within a theme, but lessons may be isolated if linked to a topic or in response to individual need.

Throughout the school year we hold various events or 'theme' days which promote digital safety e.g. Safer Internet Day and Anti-Bullying Week.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this e.g. community police officer.

Where necessary, teaching about safeguarding, including online safety, will be adapted and differentiated for vulnerable children, victims of abuse and to meet the individual needs and abilities of all pupils.

Bespoke support for specific circumstances

Due to the nature of our setting it may be that students require specific support, guidance and education around their own circumstances. This may be taught within class or delivered by the intervention team. Example interventions could be:

- Dealing with cyber-bullying
- Managing online relationships
- Healthy internet interests
- Managing screen time
- Gaming addictions
- Sexting
- Online communities chatting
- Peer to peer abuse

Resources

As technology is always evolving it is likely that many resources used will be online animations and videos. Staff will also use photographs, screen shots and activities from various trusted resource networks. The school will also use resources produced by reputable companies e.g. Google, Microsoft, School 360.

The school will not ask students or staff to bring in or use their own devices on site.

CPD

CPD will be provided throughout the year for staff, either in house or through accredited/ registered organisations. CPD will be around specific technologies the curriculum content or resources to deliver the digital safety curriculum. Staff can also source their own CPD using recognised providers such as:

- Childnet
- Internet Matters

- SWGFL (Southwest Grid for Learning)
- NSPCC
- CEOP
- Think U Know

Specific CPD for staff:

- Safer working – LADO
- Safer School culture training – HR
- E-safety training – NCC ICT/SEN Online Safety Consultant

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.

Online safety concerns will also be covered during meetings with parents.

If parents have any queries in relation to online safety, these should be raised in the first instance with the class teacher, but if urgent or of concern then the head teacher and/or the deputy DSL should be contacted directly.

Concerns or queries about this policy can be raised with the head teacher.

6. Cyber-bullying

6.1 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 support and regulation policy).

6.2 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. Class teachers will discuss cyber-bullying with their class groups as part of the Computing curriculum.

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 shares information/leaflets on cyber-bullying with 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.

6.3 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.

Monitoring and Filtering

The internet content and access is filtered through Lightspeed. The content controls and managed by NCC E-safety team.

Within school we monitor usage and content through SensoCloud. This is intelligent monitoring software which monitors all devices within school. Ant potential violations are then captured through a screen shot. Each Monday a report is sent through to the DSL and deputy DSL. Each capture will be checked and categorised depending on content.

7. Acceptable use of the internet in school

All parents, staff, volunteers, governors and, where possible, pupils are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school with the intention of them being used for their safety on their journeys to and from school. Pupils are not permitted to use mobile devices at any time whilst on the school site or engaged in school activities off site.

Staff must be made aware that pupils have a mobile device and it must be switched off and stored in a secure place during school hours unless permission has been sought to use for a specific purpose.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with school policies and procedures and may result in the confiscation of their device or a call to parents/cares to collect the device.

Publishing Information Online – School Website

Barndale House School will use e-mail, Facebook and the website as the main means of communication with parents/carers and the wider community. The information posted will always be authorised by the head teacher before

being posted online. No information will be shared online that will identify a pupil or pictures posted unless prior authorisation has been given by parent/carer.

9. Staff using work devices outside school

Staff members using a work device outside of school must not install any unauthorised software and must not use the device in any way which would violate the school's terms of acceptable use.

Staff members must take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Ensuring their hard drive and any USB devices used are 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

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 the ICT technician.

10. 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 Support and Self-regulation and Internet Acceptable Use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The head teacher and deputy receive weekly reports from Sensocloud and will follow up any reported incidents.

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 and /or Staff Disciplinary procedure. 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 or LADO.

Social Media and Professional Conduct Online

NCC provide a staff 'Social Networking Policy' which has been adopted by the Governing Body of Barndale House School. Alongside our Code of Conduct and Staff Handbook documents there is clear guidance given to staff about keeping themselves safe and preventing the reputation of the school coming into question. Some of the key aspects covered in the Social Networking Policy are:

- Clear distinction between personal business and business use of social media
- Caution over posting or sharing any personal information that may bring the school into disrepute
- It is the users responsibility to protect their own professionalism
- No contact should be made with pupils

Further information can be found on the online safety helpline:

https//swgfl.org.uk/services/professionals-online-safety-helpline/

11. Training

All new staff members will receive information, support and guidance 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:

  Cyber-bullying -Abusive, harassing, and misogynistic messages

  Online sexual harrassment

  Consensual and 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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPoms.

This policy will be reviewed every year by the head teacher. At every review, the policy will be shared with the governing board. The review 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.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Support and self-regulation
- Staff disciplinary procedures
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • 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 • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, breaktimes, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement (pupils) Adapted version

Acceptable Use Policy for Pupils

To keep everyone safe when using computer equipment at school I will:

- hand my mobile in when I arrive at school. I will get it back at the end of the day. 
- use the computers safely at all times.  
- understand that I am responsible for my own actions. I know that school software checks computer files and monitors what sites I use.
- not use other people's accounts or files.
- only use programs that are already on the school computer or I-Pad.
- report any inappropriate material messages to staff. I know I can click the CEOP button to report inappropriate material. 
- only take appropriate photographs or videos using school equipment. I will ask for permission. 
- only send e-mails with permission from my teacher. 
- remember not to share my personal information. For example, full name and address.
- not access social networks or chat rooms. 
- Remember to treat others fairly and not upset people online. 

Name of Pupil: _____ Class: _____

Signed by Pupil: _____ Date: _____

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of all technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such

communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____

Online Teaching & Learning (inc. working from home)

As part of extending the curriculum offer, Barndale House School will provide access to e-learning resources. These will enhance or extend the learning that is taking place in the classroom. The learning will be through education APPs, online links or using the School360 platform, which includes the use of emails.

No other platforms, means of communication or social media should ever be used for contact with students, parents or carers.

Online Learning Platforms and APPs

All learning platforms and APPs will be managed by Barndale House School, so that the certification and robust data protection policies can be followed. It is also important that a member of the SLT would remain an admin on all platforms and APP based learning resources.

Staff working from home

Staff working at home can choose to use their own devices, if they are confidently able to safeguard the information and use of these.

Some key information for staff working at home:

- It is essential that all usernames, passwords and log on information is easily accessible
- Any digital files required at home should be emailed or held temporarily on Googledrive so they can be uploaded back onto the secure network once back in school. ***Any items viewed/downloaded should be deleted from staffs' devices and removed from the bin.***
- No other users at home should view, be able to access or communicate school information, including information about pupils, staff and documentation
- If staff are not confident in the use of devices at home they should seek further advice
- Staff should not use any methods that have not been previously agreed by the headt eacher to complete work, transfer information or contact students/colleagues
- Staff should take care of their own mental and physical health whilst working from home

Any safeguarding concerns must be shared with the DSL and use appropriate routes to share these concerns:
phone call and CPOMs