



E Safety Policy

Ratification Date: 5/09/23

Signed: Diane Robinson/Tracey Lecointe

Review Date: 5/09/25

Introduction to E Safety

Our pupils are growing up in an increasingly complex world, living their lives seamlessly on and off line. This presents many positive and exciting opportunities, but also challenges and risks.

The use of technology is actively encouraged at the New Bridge Alternative Education but with this comes a responsibility to protect both pupils and the school from abuse of the system.

What is this Policy?

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE) and other statutory documents; it is designed to sit alongside the school's Child Protection and Safeguarding Policy.

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

Overview-Aims

This policy aims to:

- Set out expectations for all New Bridge members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care, and
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
 - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.

Scope

This policy applies to all members of New Bridge (including staff, the proprietor, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together and support each other in a world that is online and offline at the same time.

Proprietor

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff
- Undertake training in E Safety, in accordance with statutory guidance.
- Liaise with the designated safeguarding lead and online safety coordinator on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DSL, Proprietor and senior management team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. ICT technician) who carry out internal technical online-safety procedures
- Ensure the Proprietor is regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure all remote learning policies are kept up to date
- Ensure the school website meets statutory requirements.

Designated Safeguard Lead

The DSL at The New Bridge Alternative Education will take lead responsibility for Child Protection and Safeguarding (including online safety).

Key Responsibilities;

- “Liaise with the local authority and work with other agencies in line with Working Together to Safeguard Children”
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, Proprietor and senior management team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the headteacher
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with the senior management team and the designated advisory board member for child protection to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss ‘appropriate filtering and monitoring’ with the Proprietor and ensure staff are aware.
- Ensure the Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
 - all staff must read KCSIE Part 1 and all those working with children Annex A
 - it would also be advisable for all staff to be aware of Annex C (online safety)
 - cascade knowledge of risks and opportunities throughout the organisation.
 - Keep all remote learning policies up to date.

All Staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Coordinator (OSC) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for Senior management team and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main child protection and safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff code of conduct
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use policy, including the remote learning responsible user agreement for pupils, remind them about it and enforce school sanctions
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues

- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Follow the remote learning policy and teacher protocols during any part or full school closure

Pastoral Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/ Relationships Education curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE and Relationships Education.

ICT Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior management team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Volunteers, Visitors and Contractors

Key responsibilities:

- Report any concerns, no matter how small, to the designated safeguarding lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Students

Key responsibilities:

- Read, understand, sign on admission and adhere to the pupil acceptable use policy
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies (including remote learning policies) cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/Carers

Key responsibilities:

- Read, sign on admission and promote the school's parental acceptable use policy (AUP), including remote learning policies and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, Proprietor, contractors, pupils or other parents/carers.

Education and Curriculum

The following subjects have the clearest online safety links at the New Bridge Alternative Education (see the relevant role descriptors above for more information):

- PSHE and Relationships Education
- Prince's Trust Achieve Programme

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place via Securus).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At The New Bridge Alternative Education, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to focus on the key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling Online Safety Concerns and Incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of PSHE).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety coordinator / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

The school's procedures for dealing with online-safety are mostly detailed in the following policies (primarily in the first key document):

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)

The New Bridge Alternative Education commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Proprietor, unless the concern is about the Proprietor in which case the complaint is referred to another senior member of staff. Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

System Security

Monitoring

The school reserves the right to monitor the use of the network, internet and e-mail systems. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached, appropriate disciplinary action will be taken.

The school internet system has a filtering and monitoring system run by _____ which monitors and filters all website access against pre-set policies.

Property

Pupils and staff should treat any property belonging to the school with respect and reasonable care and report any faults or breakages to a member of office staff.

Viruses

Pupils and staff should be aware of the potential damage that can be caused by computer viruses. Pupils and staff must not download, install or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources.

System Security

- All computers and laptops are password protected. Passwords are changed on a regular basis.
- Pupils should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access.

- Do not make deliberate attempts to disrupt or damage the school network, any device attached to it or any data stored on it or transmitted across.
- Do not alter school hardware in any way.
- Do not knowingly misuse headphones or any external devices e.g. printers, mice.
- Do not eat or drink while using the computer.
- All users should log out of any device properly as well as ensure the device is shutdown in order to protect user data.

Leaving workstations

If a person leaves their workstation for any period of time they should log out of their workstation.

Internet

The School recognises the benefits to using the Internet in an educational environment. The Internet facility is provided for school related activities only. The school monitors the use of the Internet. Any inappropriate material, whether it be sexual, violent, extremist or illegal in nature will be blocked and the System Administrator alerted, who will in turn alert the school Designated Safeguarding Lead, as to the inappropriate material being accessed.

Viewing, retrieving, or downloading of any material that the school considers inappropriate will result in appropriate disciplinary action.

Good Practice for Staff, Parents/Carers and Pupils

Staff Personal Safety

It is vitally important that staff are careful about content that they search out or download. Every time you view a page on the internet, it is possible to trace your visit back to the school computer. This means that it is possible to tell if the school computer was being used to look at inappropriate web pages.

Staff need to ensure that films or other material shown to children are age appropriate.

Staff must be aware of their responsibilities to the school when using social networking sites such as Facebook. Our staff code of conduct and confidentiality policy must be adhered to at all times, even outside of working hours. It is important to maintain your status as a professional teacher.

Disciplinary action could result if the school is brought into disrepute.

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation.
- Staff must not post photos related to the school on any internet site including pupils, parents, staff or the school branding (uniform).
- Staff must not form online friendships with pupils and parents.
- Staff must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Staff should use their school email account for all school-related communications.

- Staff to be aware of the various members of staff responsible for Safeguarding issues
- Staff members should refer to the Staff Code of Conduct for more detailed information.

Pupils

Pupil Personal safety

- The school will organise internet safety lessons on a termly basis with one from an external presenter.
- Pupils must not play with or remove any cables etc that are attached to a school computer.
- Pupils will be taught how to stay safe when working online at school and at home.
- Pupils must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Pupils must not post anything on any online site that can be constructed to have an adverse impact on the school's reputation.
- Pupils must not post photos of video related to the school on any internet sites including pupils, staff, parents or the school branding (uniform).
- Pupils should never reveal their full name, any address or contact details, any school or network user ID or password online, even if communicating with known acquaintances.
- Pupils should be aware that the potential exists for predators to remain entirely anonymous and easily pose as someone else.
- Pupils should employ a healthy mistrust of anyone that they "meet" online unless their identity can be verified.
- The use of chat rooms and social networking sites are not permitted in school.
- Do not arrange to meet anyone you have met on the internet - people are not always who they say they are.

Parents/Carers

Parents

- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to limit the kind of content your children can access through the mobile network.
- Parents need to be aware that the parental control software doesn't replace the need for supervision and education when working on the internet.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's internet use and discuss various issues pertaining to the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.

- Parents should discuss the care needed when their children meet online "friends". Only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is really important.

You can find out more about how children use social media, the apps they use, the risks they face, how to use privacy settings, and advice and tips about how to talk to children about e-safety at;

Useful Safeguarding websites

The UK Safer Internet Centre website

<http://www.saferinternet.org.uk>

CEOP's Thinkuknow website

<http://www.thinkuknow.co.uk>

<http://www.thinkuknow.co.uk/parents>

Internet Matters

<http://www.internetmatters.org>

Childnet

<http://www.childnet.com>

NSPCC

<http://www.nspcc.org.uk/online-safety>

Parent Zone

<http://www.parentzone.org.uk>

Ask About Games (where families make sense of video games)

<http://www.askaboutgames.com>

Inappropriate Behaviour

Bullying of another person will be treated with the highest severity.

Online, Cyber Bullying

- Lessons concerning cyber bullying to be carried out termly through curriculum.
- By cyber bullying, the School is referring to: bullying by email, messages, images, calls or other electronic communication.
- Use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites (including social networking sites).
- Hijacking or hacking email accounts.
- Making threatening, abusive, defamatory, or humiliating remarks in chat rooms or on instant messaging services.
- The use of social media for the use of bullying, grooming, abuse and radicalisation.

Pupils should be aware that cyber bullying is generally criminal in character and that English law does apply. The School will endeavour to resolve all matters using the School's Behaviour Policy without Police involvement but parents of victims do have the right to seek Police intervention. This will be closely linked to the School's Anti-Bullying Policy and The New Bridge Alternative Education Child Protection and Safeguarding Policy which can be read separately or in conjunction with this policy.

Have Concerns as a Parent?

Before doing anything, take a deep breath and remain calm. There's lots of information and advice on the <https://www.thinkuknow.co.uk/> site to keep your child safe and access support.

Having a calm and open conversation is one way for you and your child to explore what is happening in an honest and supportive way.

Discuss your concerns with someone you trust, for example a friend, partner or the school.

You can also talk to a professional at the NSPCC helpline on 0808 800 5000.

Talking about it will help decide the best action to take to ensure your child is safe.

TO MAKE A REPORT

If you are concerned about online grooming or sexual behaviour online you can contact CEOP: <http://www.ceop.police.uk> or alternatively you can click on the 'Report Abuse' button located at <https://www.thinkuknow.co.uk/>

If you stumble across criminal sexual or obscene content on the internet you should report it to the Internet Watch Foundation: <http://www.iwf.org.uk>.

You can also report directly to your local police force.

If you think your child is in immediate danger call 999

Email

Personal use

Email is provided for school related purposes only. The school monitors the use of email and disciplinary action may be taken if inappropriate uses of personal emails are discovered.

Status

Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. Pupils and staff should not include anything in an email that is not appropriate to be published generally. Any email message which is abusive, discriminatory on grounds of sex, race, disability, sexual orientation or religious belief, or defamatory is not permitted.

Privacy

All files and emails on the system are property of the The New Bridge Alternative Education. As such, system administrators and staff have the right to access them if required.

Secure Documents

All emails of a sensitive or secure nature should be sent using the 'Egress' email system. Staff can find out about this by talking to a member of the Safeguard Team.

Plagiarism and Copyright

Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the internet or anywhere else.

You should respect copyright. Breaking copyright laws occurs when you reproduce a piece of work that is protected by copyright. If you are unsure whether or not you can use a piece of work, you should request permission from the copyright owner. This includes the copying of music files, DVDs and CDs. The New Bridge Alternative Education purchases appropriate licences where required.

Digital Images and Video

The word photography is used in this policy to include traditional photographs and digital images of any kind, still or moving.

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used.

Photography and video are familiar features of life, playing a significant role in commerce, entertainment and communication; it is commonplace in our homes and it is an important element of school life.

At New Bridge Alternative Education we feel it is vital that achievements are recognised and that pupils feel valued, proud and happy. Photography is a useful tool within school and it is

employed routinely in many ways, for example; record keeping, displays, special events, teachers' lessons and the children's own work.

On occasions photos are also used for the Press, school website, school social media pages and other promotional purposes.

Children will only be named in photographs that are displayed within the school. We will not provide children's full names for any other purpose unless special parental consent has been received.

We are, however, sensitive to the wishes and rights of parents who may not wish their children to be photographed and who may have concerns about the use of such images

Taking Photographs and Video

All parents are asked to give consent for photography of their child by completing a permission slip that is contained within the Admission Pack. A record is kept of children who must not be included in press, website or any other photographic image, still or moving.

All reasonable measures will be taken to ensure that no child on the register is photographed or videoed by a visitor to school or while on an educational visit outside school.

From time to time we may invite the Press into school to share special events and achievements within the local community. We will allow local newspapers to take photographs of children, when appropriate, provided that parental consent has been given.

Some newspapers insist that children's names must be published with their photographs. If not, they may decline to cover school events. Therefore, we will normally give the children's full names (but not addresses) to newspapers only if requested by them. That is why it is important for you to tell us whether you have any objections.

Images Taken by Edge Staff

The printing of images is always carried out on the school premises. Any photographic images held on staff phones must be deleted at the end of day.

All images taken must be deemed suitable without putting the child in any compromising positions that could cause embarrassment or distress.

Photographs taken as records of events or for educational purposes may be displayed around the school. They are then archived or shredded after use.

Photographs are not exchanged with anyone outside school, or removed for private use by any employee or volunteer.

Images Taken by Children

The school encourages children to take photographs on school trips or visits as a way of recording events.

There is no reason why pupils should not be allowed to take photographs so long as anyone photographing respects the privacy of the person being photographed. This is seen as part of the school's code of behaviour.

Infringement of this respect of privacy is akin to bullying and will be dealt with in the same way as any other breach of school discipline.

Should the school learn about any inappropriateness of image use involving our pupils or staff, we will immediately act and report it as we would for any other child protection issue.

Social Media

The New Bridge Alternative Education works on the principle that if we don't manage our social media reputation then someone else will.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Staff, Pupils' and Parent/Carers Media Presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online

behaviour, how to be a good friend online and how to report bullying, misuse, intimidation, or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Email is the official electronic communication channel between parents and the school.

Pupils and parents are not allowed* to be 'friends' with or make a friend request** to any staff, volunteers and contractors or otherwise communicate via social media.

Pupils and parents are discouraged from 'following' staff, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

* Exceptions may be made, e.g., for pre-existing family links, but these must be approved by the Principal, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Proprietor (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on digital Images and video.

Use of Mobile Phones

Pupils

Students are encouraged to use their phones responsibly and allowed to keep it in their possession. This privilege is removed if breeched and phones placed in a secure locker.

Staff

- The school accepts that employees will bring their mobile phones to work.
- Mobile phones and personally owned devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
 - Employees are encouraged to not make/receive calls/texts during lessons or formal school time

- Staff should use phones in designated safe areas. If a private call needs to be made then a request for a room can be made to the Principal / Proprietor
- If a staff member breaches the school policy then disciplinary action may be taken as appropriate.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.

Acceptable Use Policy (AUP) (signed on entry in Admission Pack)

The school's ICT systems and network are provided to assist you in your studies.

As a student at New Bridge Alternative Education, you are bound by the terms in this policy:

1. I will only access the system with my own login and password, which I will keep secret.
2. I will not access other people's files.
3. I will only use the computers for schoolwork, homework and related tasks.
4. I will not use USB sticks from outside school unless I have been given permission.
5. I will not visit internet sites that I know may contain material of an unsuitable nature.
6. I will respect copyright rules whilst using the computer systems.
7. I will not post or forward anonymous messages on the network internet.
8. I will not download material of the internet unless it's appropriate to my studies.
9. I will not give my home address, telephone number, or arrange meetings without permission.
10. I will report any unpleasant material or messages sent to me.
11. I understand that my actions on school computers are scrutinised by monitoring software.

When using the school ICT communication and collaboration facilities I must:

1. Respect other people's views and beliefs.
2. Post comments which are appropriate to the discussion.
3. Must NOT post anything abusive, obscene or illegal on any area of the network.
4. Must NOT include material which is confidential, or copyright protected without permission.

I understand school will check my computer files and monitor sites I visit, and that use of the system without permission or for purposes not agreed could constitute a criminal offence under the Computer Misuse Act 1990.

New Bridge Alternative Education reserves the right to remove, vary or amend any of the content which appears on the network at any time and without prior notice. Furthermore, I understand that the school reserves the right to administer its own sanctions if part or any of the above agreement is broken.

STUDENT

I understand and will abide by the provisions and conditions of the ICT acceptable use policy. I understand that any violations of the provisions may result in disciplinary action and the revocation of my privileges. I also agree to report any misuse of the system to a staff member. Misuse may come in many forms but may be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal activities, racism, sexism, inappropriate language, any act likely to cause offence, or other issues described above.

Signature

PARENT**or****CARER**

As the parent or Carer, I have read this agreement and understand that access to electronic information services in school is designed for educational purposes. I understand that, whilst the Internet service provider operates a filtered service, it is impossible for New Bridge Alternative Education to restrict access to all controversial materials and will not hold the school responsible for materials acquired on the network. I also agree to report any misuse of the system to the school.

I hereby give my permission to New Bridge Alternative Education to give my child access to electronic information services and I certify that the information given on this form is correct.

Signature

Date