Brinsworth Manor Junior School

Acceptable Use Policy

Name of school	Brinsworth Manor Junior School
Policy review date	October 2017
Date of next review	September 2018
Who reviewed this policy?	SLT
Version Number	2.1

Contents

Introduction

In order to exploit the many educational and social benefits of new and emerging technologies, learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. At times, they will encounter risks.

We now recognise, however, that Online Safety risks are posed more by behaviours and values online than the technology itself. Our approach must therefore change: rather than restricting access to technology, we need to empower learners to develop safe and responsible online behaviours to protect them whenever and wherever they use technology. Acceptable Use Policies (referred to as AUP's throughout this document), when embedded within a wider framework of Online Safety measures, can help to promote the positive behaviours needed.

Online Safety is about enabling an institution to benefit as much as possible from the opportunities provided by the Internet and the technologies we use in everyday life. It's not just about the risks, and how we avoid them; it's about ensuring everyone has the opportunity to develop a set of safe and responsible behaviours that will enable them to reduce the risks but still access the benefits.

Schools and other establishments are increasingly recognising the benefits of technology and particularly social networking as an essential component of productive and creative social learning. However, in doing so, they are finding that a 'blocking and banning' approach which merely limits exposure to risk is no longer a sustainable approach. Ofsted's recommendation is that learning environments move towards 'managed' systems with fewer inaccessible websites. This should be accompanied by teaching and learning that equips children and young people to manage online space positively and safely.

Children and young people will experiment online, and while their confidence and enthusiasm for using new technologies may be high; their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter. Educational establishments now need to focus on a model of **empowerment**: equipping children and young people with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they use technology

Aims of this Policy

This policy is designed for use by everyone in our school community.

The key priorities of this policy are:

- To ensure the safeguarding of all children and young people within and beyond the educational setting by detailing appropriate and acceptable use of all online and offline technologies.

- To outline the roles and responsibilities of everyone involved.

- To ensure everyone is clear about procedures for misuse of any online and offline technologies both within and beyond the educational setting.

- To develop links with parents and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues.

- To clearly state what is acceptable and unacceptable behaviour online.

What is an AUP?

AUP is an acronym for Acceptable Use Policy; at its most basic level, it is a document usually in the format of a poster which sets out the way in which users of ICT should and should not make use of the systems provided to them, including using the Internet. AUP posters should be displayed in prominent locations in the vicinity of ICT environments, notice boards, website or Intranet.

Why are AUPs important?

AUP's demonstrate how work has been achieved to create a balance between using ICT to enhance learning and teaching, and putting appropriate safeguards in place at the same time.

AUP's are an important way of encouraging all members of the community to take responsibility for their own safety when using technology. Effective AUPs can help to establish and reinforce safe and responsible online behaviours both in an educational environment as well as in the home where many inappropriate behaviours go undetected.

AUP's are also an effective means of protecting an organisation by ensuring that all users of ICT are aware of the consequences and actions of inappropriate behaviour or malicious intent. AUPs are also designed to protect staff from any unwarranted accusations from either staff or children and young people. For example, some staff may be unaware that contacting or responding to a child or young person through personal channels (such as a private social networking account) is inappropriate which could lead to investigation, either as an internal matter by their employer and / or the Police.

Who is responsible?

Online Safety is an important aspect of strategic leadership within the educational setting and key stakeholders have ultimate responsibility to ensure that policy and practices are embedded and monitored.

This policy, supported by the AUP's for staff, Governors, visitors and children and young people is available to protect the interests and safety of the whole learning community.

Schools and other educational settings

It is the overall responsibility of Head teacher with the support of the Governing Body and staff to ensure that there is an overview of Online Safety (as part of the wider remit of Child Protection) across schools and to implement this policy or an adaptation of it.

Staff and other adults

It is the responsibility of all adults within a school or other educational setting to:

- Ensure that they know who the designated person for Child Protection is within the school or other setting so that any misuse or incidents can be reported which involve a child or young person. Where an allegation is made against a member of staff it should be reported immediately to the nominated Child Protection Officer and recorded.

- Be familiar with Behaviour, Anti-bullying (including online bullying) and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately.

- Ensure that children and young people are protected, educated and supported in their use of online and offline technologies. They should know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.

- Be up-to-date with Online Safety knowledge and be equipped with Online Safety training skills (where applicable) that are appropriate for the age group and reinforce this through the curriculum.

- Sign an AUP to demonstrate that they agree with and accept the rules for staff and other adults using ICT. All staff should receive a copy of the AUP which must be signed and retained on file. The AUP should be displayed in a prominent area (e.g. Staff Room) to serve as a reminder that staff and other adults have an equal responsibility in the safe use of ICT.

- Use ICT in an appropriate way that does not breach the Data Protection Act 1998 and other relevant and associated legislation.

Children and young people

Children and young people should be actively encouraged to become involved in the review of this policy through a School Council or other similar forum, in line with this policy being reviewed and updated.

In addition, children and young people should be;

- Responsible for following the AUP rules whilst within an educational setting commencing from the beginning of each academic year or whenever a new child or young person attends a school or similar setting for the first time.

- Taught to use the Internet (including mobile phones that can access the Internet) in a safe and responsible manner through ICT, PSHE, clubs and groups, Citizenship or collapsed timetable days on Online Safety.

- Taught to have the confidence to inform an adult about any inappropriate materials or contact from someone they do not know immediately, without reprimand (age and activity dependent).

The AUP and the accompanying letter for children and young people and parents are provided in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school and other educational settings.

The AUP should be prominently displayed within the school, where appropriate, so that it provides a constant message at all times.

Parents

Parents can play a vital role in supporting this policy with their child, which is demonstrated by discussing and signing the AUP together so that it is clear to the school or setting, that the rules are accepted by the child or young person with the support of the parent. (There is no statutory requirement for parents to sign AUP's but evidence shows that children and young people signing agreements to take responsibility for their own actions, is largely successful.)

The AUP is also intended to provide support and information to parents when children and young people may be using technology beyond an educational setting (i.e. Home environment).

Security and Privacy

Passwords

It is recommended that this standardised password policy is adopted in line with BECTA standards:

Length	Complexity	Lifespan (staff)	Lifespan (students)
8	Yes	90 days	365 days

- Depending upon the age group and setting, users may be provided with a unique individual network, email and Learning Platform log-in username and password.

- It is important to ensure that any passwords belonging to users are kept private and not shared with anyone else. Passwords should never be written down.

- If a user suspects that their password has been accessed and has been used by someone to access the network, this should be reported to a member of staff immediately.

- Likewise, passwords must never willingly be shared with anyone else. If the network is accessed and used inappropriately by someone pretending to be another user, it may mean that the default user could be held responsible for any actions as it will be difficult to prove misuse otherwise.

- It is good practice for users to be responsible with their personal log-in details which will help them to remain vigilant when using other systems including home environments.

- It is also good practice to end a session by logging off correctly or when temporarily moving away from the computer. Users should attempt to get into the habit of doing this each time the computer is left unattended so that no one else can use the open session. It is only a small inconvenience to log back in again.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of networks and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users or administrators must also make sure that workstations are not left unattended and are locked.

eMail

The use of email within most environments is an essential communication tool for adults, children and young people. Educationally, email can offer significant benefits. For example; direct written contact between establishments on different projects, be they staff based or pupil based, within school, national or international.

It is recognised that all email users need to understand how to style an email appropriate to their skills, experience, age and understanding.

All users provided with an email account should follow these basic principles of good practice guidelines and in line with school or other educational setting's policies:

- Staff are usually provided with their own email account to use for all educational business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed to anyone else.

- It is the responsibility of each email account holder to keep their password secure. For the safety and security of users and recipients, all email is filtered and logged; if necessary, email history can be traced.

- Under no circumstances should staff contact children and young people or parents or conduct any work related business using personal email addresses.

- Rotherham Grid for Learning email (RGfL) provides a standard disclaimer that is attached to all email correspondence as follows:

The information in this e-mail is confidential and intended solely for the use of the individual to whom it was addressed. If you are not the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please advise the sender by using the reply facility in your e-mail software, and then delete it from your system. Rotherham Schools may monitor the content of the e-mails sent and received via its network for the purposes of ensuring compliance with the law and with Rotherham schools policies. Any views or opinions presented are only those of the author and not those of Rotherham Schools.

Essentially, the above example statement protects the email account holders' organisation from inappropriate use by the user and helps to prevent any unnecessary unauthorised use of any outgoing email by intended or unintended recipients.

- Email sent to an external organisation should be written carefully and professionally before sending. An email is a record in the same way that a letter is written on headed paper. The same rules apply equally to emails sent internally.

- Students may only use approved email accounts on the network and only under direct supervision (where appropriate) for educational purposes.

- The forwarding of chain letters is not permitted. Any other type of email received that appears to be inappropriate or of concern should be discussed with a member of staff.

- All email users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

- Staff must inform an Head, OnlineSafety coordinator or Line Manager/Supervisor if they receive an offensive email.

Data Security

Personal information is defined by the fact that an individual could be identified from that information. This means that data items such as name, address, date of birth, telephone numbers and even images should be handled appropriately. In isolation, some of these items may not be of concern and would not necessarily identify an individual. However, there is a risk that an amalgamation of several data items may identify an individual and therefore could lead to inappropriate disclosure of personal details.

It follows that data containing personal information needs to be treated with care. The Data Protection Act 1998 contains 8 enforceable principles of good practice which should be adhered to at all times when using, storing, accessing and sharing personal information: Personal information must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date

- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

If personal details are not kept secure, it may lead to that individual becoming exposed to risks such as fraud, theft and even their personal safety could be compromised.

For further information about the rules around Data Protection, please refer to Rotherham Borough Council's Data Protection Policy: (particularly section 7.7)

It is important that users do not access folders and files on a computer or network area that they do not have permission to use. The Computer Misuse Act 1990 makes it an offence to access material without the system owner's permission.

Before attempting to plug in portable media devices, ensure that you have the permission of a member of staff or an administrator. Devices such as digital cameras, USB memory sticks, CD's/DVD's, mobile phones, MP3 players and even personal laptops may contain viruses that could be a potential threat to a computer or network.

If you are working with data and images of other individuals, care must be taken not to save onto any removable device without either the permission of the individual/s or a member of staff. If the device is stolen or misplaced, personal information may be disclosed and this would constitute a security breach which will be investigated.

Internet

This policy (for all staff, Governors, visitors and children and young people) are inclusive of both fixed and mobile internet technologies which includes desktop PCs, laptops, notebooks, netbooks, personal digital assistants (PDAs), tablets, smart watches, webcams, interactive whiteboards, voting systems, digital video equipment and technologies owned by children, young people and staff such as laptops, mobile phones, digital cameras, PDAs and portable media players, etc.

The Internet is an open communication medium, available to most people, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young or vulnerable people.

These risks may include:

- Commercial issues with spam and other inappropriate email.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file sharing via the Internet or any mobile device.
- Viruses.
- Online-bullying.
- Online content which is abusive, harmful (pro-suicide, eating disorders, etc.), pornographic, or otherwise illegal (such as promoting terrorism, gangs or weapons).

All users of the Internet should follow these basic principles of good practice guidelines and in line with other established policies:

- All use of the RGfL network and other similar networks is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected, it will be investigated and appropriate action taken.

- The school or other educational setting maintains that students will have supervised access to Internet resources (where reasonable) through fixed and mobile internet technology.

- Staff should review any recommended Internet sites before use in addition to those that are currently disallowed through existing filtering software.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by a member of staff. It is advised that parents recheck these sites and supervise this work where this is practical or reasonable.

- All users must observe software copyright at all times. It is illegal to copy or distribute software from other sources.

- All users must observe copyright of materials including text and images.

- Schools and other educational settings should be aware of its responsibilities when monitoring communication under current legislation such as the Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998. The School or other educational setting will not monitor staff except in specific situations where misconduct or misuse is suspected, but it should be noted some systems designed to monitor the safety of students may not be able to discriminate between staff and student logons.

- If staff or children and young people discover an unsuitable site, the incident should be reported immediately to an appropriate member of staff.

- It is the responsibility of the school or other educational setting by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up-to-date on all ICT equipment.

- Users are not permitted to download programs or files without seeking prior permission from a member of staff or Network Manager.

- If there are any issues related to viruses or anti-virus software, a member of staff or the Network Manager should be informed.

Currently the Internet technologies children and young people are using both inside and outside of the learning environment include:

- Websites
- Learning Platforms and Virtual Learning Environments (VLE's)
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functions
- Other mobile devices with web functionality

Whilst the Internet can be both beneficial and exciting in and out of a learning context, it is not consistently policed largely due to the fact that it is impossible to do so. All users need to be aware of the range of risks associated with the use of Internet technologies.

It is also important that staff and other adults are clear about procedures, for example; only contacting children and young people about homework via a school email address or school telephones, not personal email addresses or mobile phone numbers, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst a school or other educational setting acknowledges that they will endeavour to safeguard against all risks, they may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people are protected.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smartphones and smartwatches are familiar to children outside of an educational setting too. They often provide a collaborative, well known medium with possible Internet access but equally, they expose risk and misuse associated with communication and Internet use.

Emerging technologies should be examined for educational benefit and the risk assessed before use is allowed.

Schools and other educational settings should manage the use of these devices in the following ways so that users exploit them correctly and appropriately:

- Staff and other adults are allowed personal mobile phones and other devices for their own use. Under no circumstances should a member of staff contact a pupil or parent using their personal phone.

- Staff mobile devices (including mobile phones and tablets, etc.) should not be accessible to children. They should be kept out of sight during times when children are present. Mobile devices should be protected using a passcode or similar security measure to prevent unauthorised access.

- The school or other educational setting is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate or threatening text messages between any members of the community (within or outside an educational setting) is not allowed and may result in a serious offence being committed.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

- The school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

- The school provides desktop PCs and laptops for staff, only these devices may be used to conduct educational business outside of the educational setting.

Social Networking

Social networking sites (Facebook, ,Twitter, etc.), if used responsibly both outside and within an educational context can provide easy to use, creative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, staff, other adults, children and young people should think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

One of the key benefits of social networking sites is that they encourage children and young people and adults to be creative users of the Internet. They can express themselves with an online personality, use all the applications the site has to offer, chat and socialise with peers, and share multimedia content such as music, photos and video clips with others.

There are concerns that staff, other adults and children and young people may upload content that is inappropriate, offensive or even illegal to their online spaces, posting material that could damage their reputations or the reputations of others. Equally they may post inappropriate comments to the profiles of others, which can result in bullying, slander or humiliation of others.

Many adults, children and young people maintain very detailed online profiles, including a large amount of personal information, photos and accounts of daily routines which could lead to them being identified or contacted in person. The contact risks of other forms of new technology are well documented, and those that seek to harm or exploit children and young people will use social networking sites as another way to contact and groom potential victims. Most social networking sites do contain privacy settings, allowing a profile to be set to private and only viewed by approved contacts, but these are not always used. Indeed, one of the big attractions of social networking sites is the large numbers of 'virtual' friends that can be linked from a profile, but this can expose adults and children and young people to the risks of unwelcome contact.

Staff may also put themselves at risk of online bullying by placing too much personal information on social networking sites that can be used against them by disaffected members of the school community.

At present, access is denied to social networking sites to staff and children and young people within an educational setting unless a clear business need has been granted. (Staff may only create blogs, wikis or other spaces in order to communicate with children and young people using the Learning Platform or other systems that have been approved.)

The following advice and good practice guidance should be followed in order to stay safe whilst using social networking sites:

- All staff, other adults, children and young people are advised to be cautious about the information given by others on sites. For example; users not being who they say they are.

- Users should avoid placing images of themselves, family, friends or colleagues or details (metadata) within images that could reveal background information on such sites and to consider the appropriateness of any images posted due to the difficulty of removing an image once posted online.

- Users should avoid giving out personal details on such sites which may identify them and their whereabouts (full name, address, mobile/home phone numbers, school details, email address, specific hobbies/interests, etc.).

- It is advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

- Users are encouraged to be wary about publishing specific and detailed private thoughts online.

- Report any incidents of bullying (including cyberbullying) to an appropriate member of staff including any material or instructions you are uncomfortable with.

- Staff and other adults must never use social networking sites to contact children and young people outside of an educational environment even when considering replying to a message or invitation. The intention may be completely innocent, but this would be very difficult to prove in the event of the action being reported.

- Children and young people must never use social networking sites to contact staff or other adults in an educational setting using personal profiles whilst in a private or home environment. Communication should be made within an educational networking environment (For example, homework messages). Social networking sites of any kind should never be used to embarrass, upset or bully staff, other adults or children and young people.

- All users' must abide by the terms and conditions of social networking sites and must never create false profiles including age.

Images

Digital images are easy to capture, reproduce and publish and, therefore, easy to misuse. We must remember that it is not always appropriate to take or store images of any member of the educational community or public, without first seeking permission and considering the appropriateness or consequences. An image that identifies a living individual or individuals is regarded as personal data as defined by the Data Protection Act 1998 in the same way that written data is. It is important that the following statements are adhered to:

- With the written consent of parents, (on behalf of children and young people) appropriate capture of images by staff and other children and young people is permitted.

    - Staff, children and young people are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of children and young people or staff. This includes when on field or residential trips. However, with the express permission of the Head teacher or other suitable member of staff, images can be taken provided they are transferred immediately and solely to the network and deleted from the device. There are exceptions to these rules; children and young people may wish to capture and keep images for personal use and this is permitted providing that the subject/s is/are aware and has given permission to be filmed or photographed. A Head teacher or supervisor may use their discretion as to whether mobile phones or cameras are permitted on trips at all and the decision should be documented.

Consent of staff and other adults who work at a school

Permission to use images of all staff who work at the school should be sought on induction and a copy should be retained on their personnel file.

Publishing children and young people's images and work

Parents will be given the opportunity to grant permission (via a consent form) to enable their child's work/photos to be used in the following ways:

- on a website
- on a Learning Platform / VLE
- in a prospectus and other printed publications
- recorded / transmitted on a video or webcam
- in display material that may be used in communal areas
- in display material that may be used in external areas, e.g. exhibitions
- general media appearances, e.g. local or national media / press releases, etc

The consent form is considered valid for the entire period that the child or young person attends a school or other setting unless there is a change in circumstances. Parents may withdraw permission, in writing, at any time.

Children and young people's names will not be published alongside their image and vice versa unless prior permission is sought. Email and postal addresses will not be published particularly alongside images in connection with the individual.

Schools and other educational settings should be mindful not upload students work that may be copyright e.g. music, photographs, etc.

School website

The uploading of images to an educational website will be subject to the same acceptable rules as uploading to any personal online space. Permission should always be sought from the parent prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

Webcams, video conferencing and CCTV

- A school or other educational setting should use Closed Circuit Television (CCTV) for security and safety appropriately and according to data protection principles. (Rotherham MBC CCTV Policy and Guidance):

- Webcams should only ever be used for specific and direct learning purposes.

- Misuse of webcams by any member of the community will result in sanctions (as listed under the 'inappropriate materials' section of this document).

- Where web cams are used, consent should be sought from parents and staff in the same way as for all other images.

Video hosting sites

Images and video can be posted to blogs and social networking sites and sent by email and mobile phone. There has been a tremendous rise in the popularity of video hosting sites, such as YouTube, where clips are uploaded and shared. Popular video clips can be seen by hundreds of thousands of visitors to the sites, and clips are rated by viewers, and comments (including video comments) can be posted about them. The video footage can also be embedded in other sites and pages.

There can be a lot of useful content to view on these sites; music videos, amusing clips and other entertainment, as well as useful resources, including educational resources. Even Internet safety and anti-bullying videos can be found on these sites. Video is stored on and streamed from the sites themselves, which means that viewing is very easy.

There are two ways that children and young people may be exposed to risk on video hosting sites: accessing inappropriate material (e.g. violent, pornographic or illegal content) and they may post inappropriate material, which might make them contactable and vulnerable or which might lead to embarrassment for themselves or others.

Video hosting sites can be misused for online bullying, and staff as well as children and young people have been victim to content posted upon such sites. Online bullying may take the form of video taken without the subject's knowledge, even from within an educational environment that is then posted and shared.

- Under no circumstances should images, sound or text be used to cause embarrassment, upset or used to threaten anyone both in an educational setting or private environment as this may lead to sanctions placed upon the individuals and may possibly lead onto criminal prosecution.

Behaviour and respect (Behaviour and Anti Bullying Policies)

Refer to the Behaviour Policy (including anti bullying) for procedures in dealing with any potential bullying incidents via any online or offline communication, such as mobile phones, email or blogs.

All behaviours should be regarded as and dealt with in exactly the same way, whether online or offline and this needs to be a key message which sits within the ICT and PSHE curriculum for children and young people and their parents. People should not treat online behaviours any differently to offline behaviours and they should have exactly the same expectations for appropriate behaviour.

It is only the tools and technology that change, not the behaviour of children, young people and adults.

Allegation procedures involving staff and other adults

Please refer to the Child Protection Policy where applicable or the Online Safety incident flowchart (see Appendix 1) in order to deal with any incidents that occur as a result of using personal mobile or email technologies which may result in an allegation of misuse or misconduct being made by any members of staff or children and young people about a member of staff.

- Allegations should be reported to the Head teacher, manager or other member of staff immediately as appropriate or to the Chair of Governors in the event of the allegation made about the Head teacher.

- Personal equipment belonging to staff and other adults should not be used when contacting children and young people about homework or any other school issues either in or beyond an educational setting and any such action should be dealt with immediately.

- We follow this guidance to protect staff members from potential allegations of misconduct by a child, young person or parent.

External websites

In the event that a member of staff finds themselves or another adult on an external website of any type as a victim, they are encouraged to report incidents to the Head teacher and unions, using appropriate internal reporting procedures.

Disciplinary procedure for all education based staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online and offline technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the AUP in line with any staff code of conduct.

Complaints relating to staff and children and young people

- Complaints relating to acceptable use should be made to an Online Safety coordinator, Head teacher or Line Manager/Supervisor where appropriate. Incidents should be logged (see Appendix 2) and the flowchart for managing incidents should be followed (see Appendix 1).

- For less serious incidents*, it may not be necessary to take any action by using the Online Safety incident flowchart. If you witness, or are informed of anyone acting inappropriately, you should politely remind them of the AUP and any other rules depending on the circumstances and environment.

- If you do not want to approach the user or are unsure of the seriousness of the incident, or the incident has been reported after the user has left, you should report the incident to a senior member of staff who will progress the matter as appropriate and where necessary.

- Where children and young people have breached the conditions of the AUP, any misuse may be reported to the parent depending upon the seriousness of the incident.

*Less serious incidents may be: a user being heavy handed with ICT equipment; volume of equipment too loud; disruptive or loud behaviour; Spilled food or liquid damaging equipment.

Managing an OnlineSafety Incident

Reporting

All Online Safety incidents should be reported to the OnlineSafety coordinator or Head, who will log them and decide on appropriate action. This may include involvement of senior staff and leaders within the educational setting. External agencies, such as the Rotherham Safeguarding Children Board (RSCB), the Police or another appropriate agency, may also need to be notified.

Managing your response

No two Online Safety incidents will be exactly the same and should therefore be dealt with and judged on their own merits. Different Online Safety incidents will require different approaches.

In managing the response, this AUP should be referred to as it clearly defines what is ‘inappropriate’ in various Online Safety scenarios, and the sanctions that will apply.

Refer to the Appendices 1 and 2 to assist with the decision and record making process when responding to all incidents.

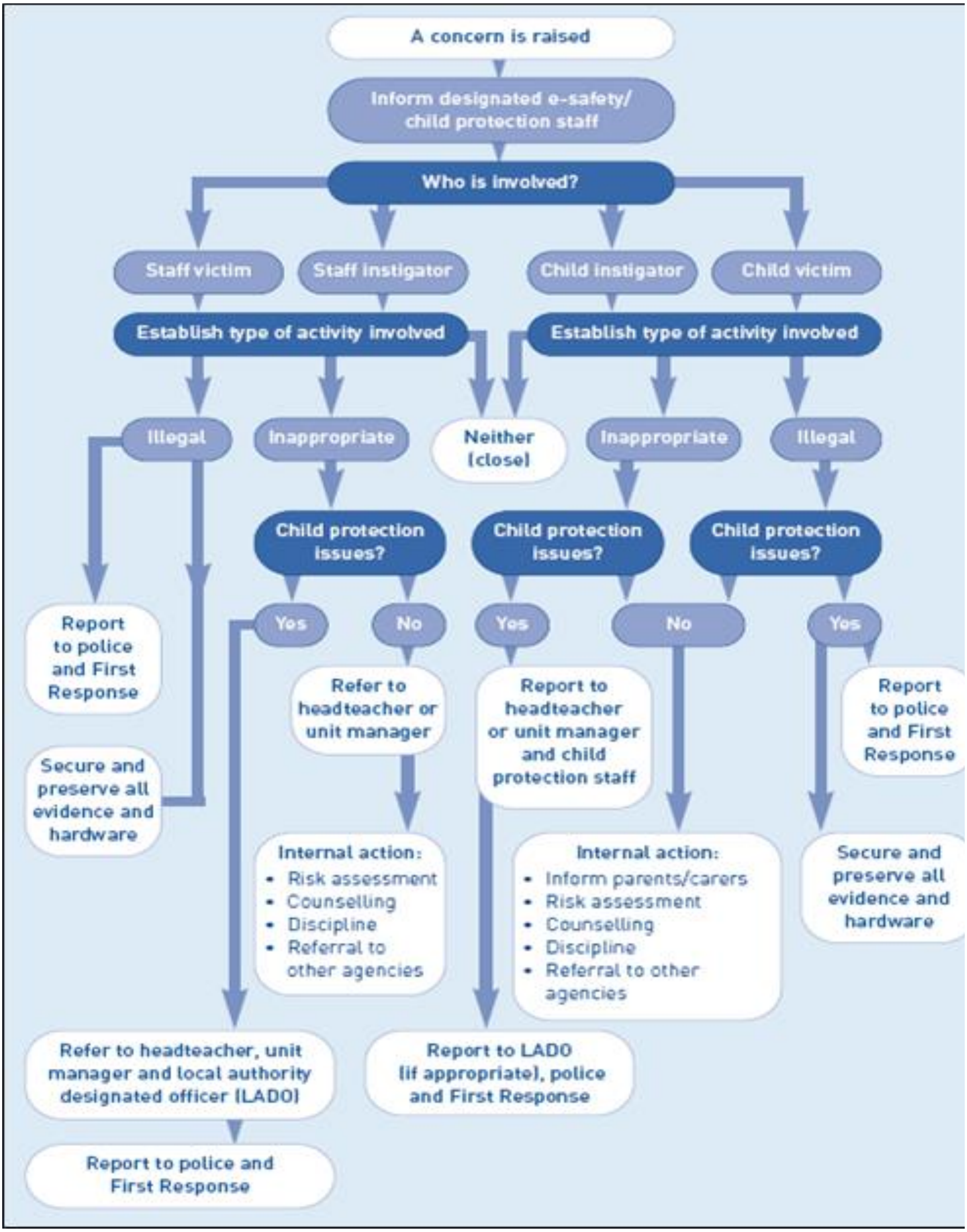
Review procedure

This policy will be reviewed every 12 months and consideration given to any comments or suggestions received for future versions. It is anticipated that any new version will be made available and educational settings informed when the time arises.

The policy will also be amended to reflect when new technologies are adopted or Central Government change any orders or guidance in any way.

Appendix 1

Flowchart for managing an Online Safety incident



A concern is raised
Inform designated e-safety/ child protection staff
Who is involved?
Staff victim
Staff instigator
Child instigator
Child victim
Establish type of activity involved
Establish type of activity involved
Illegal
Inappropriate
Neither (close)
Inappropriate
Illegal
Child protection issues?
Child protection issues?
Child protection issues?
Yes
No
Yes
No
Yes
Report to police and First Response
Secure and preserve all evidence and hardware
Refer to headteacher or unit manager
Report to headteacher or unit manager and child protection staff
Report to police and First Response
Internal action:
• Risk assessment
• Counselling
• Discipline
• Referral to other agencies
Internal action:
• Inform parents/carers
• Risk assessment
• Counselling
• Discipline
• Referral to other agencies
Secure and preserve all evidence and hardware
Refer to headteacher, unit manager and local authority designated officer (LADO)
Report to LADO (if appropriate), police and First Response
Report to police and First Response

Appendix 2

Online Safety Incident Log

Date of incident:	
Member of staff reporting incident:	
URL, (web address) of incident:	
Copy of screens/evidence saved to:	
Location of incident (room):	
Computer number if known:	
Details:	
Passed to:	
Action taken	

Appendix 3

Acceptable Use Agreement

Acceptable Use Agreement:

All Staff, Volunteers and Governors Agreement Form

This agreement covers use of all digital technologies in school: i.e. e-mail, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will follow the separate Online-safety policy (including mobile and handheld devices).I understand that this is available on the school website and in the staffroom.
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will comply with digital security policies and not disclose any passwords provided to me by the school or other related educational settings.
- I will follow 'good practice' advice in the creation and use of my password (found in the full acceptable use policy). If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access e-mail / Internet / intranet / network or other school systems, or any other school system I have access to.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network / information security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that my social media (Facebook, Twitter,instagram etc.) accounts are set to the highest privacy levels.
- I will not add as a friend (or similar) any pupils or parents of pupils (past or present) on my social media accounts.
- I will only use the school approved e-mail system(s) / communication systems for any school business, including communication with parents. This is: *RGFL Staff Mail.* I will only enter into communication regarding appropriate school business.
- I will not browse, download or send material that could be considered offensive, illegal or discriminatory.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to a member of the Senior Leadership Team.
- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission.
- I will not connect any device (including USB flash drives) to the network that does not have up-to-date anti-virus software and encryption software, and I will keep any 'loaned' equipment up-to-date, using the school's Sophos anti-virus and other digital 'defence' systems.
- All images, videos, audio and other school related data must be created, edited and stored on a school-owned device.

- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home (see exception below).
- In exceptional circumstances (eg. Camera breakdown whilst on a school trip) I am permitted to use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff provided that this use is reported to an SLT member at the earliest opportunity.
- Any images or videos must be transferred to the school network within 24 hours of them being created and any copies on the personal device must be deleted. Any images or videos found on a personal device after 24 hours has passed will be considered inappropriate and a breach of this policy.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff-only drive within school.
- I will follow the school's policy on use of mobile phones / devices at school and will not use them when children are present. I will ensure that my mobile devices are protected using a passcode or similar security measure.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities, and that I will notify the school of any "significant personal use", as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption, and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information that is held within the school's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the school's child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I will only use any other/LA system I have access to in accordance with its policies.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that all Internet usage and network usage can be logged, and that this information can be made available to the Head / Safeguarding Lead on their request.
- *Staff that have a teaching role only:* I will embed the school's Online safety / digital literacy curriculum into my teaching.

Acceptable Use Agreement Form: Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and that I read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ....Date..

Full Name .... (printed)

Job Title / Role

Appendix 4

Child-friendly Acceptable Use Policy

We know that it is important to follow this agreement to keep us safe and to treat ICT equipment with care. If you need help or are unsure about anything written below, please ask a member of staff. Any breach of the conditions below may lead to withdrawal of your access to ICT and the network.

Passwords

- I will only use my class ID and password to log onto a computer.
- I will not give out my password to anyone.
- I will log off properly after I have finished with the computer.

Data Security

- I will never give out personal information to anyone.
- I will ask before using portable media (like memory sticks) on the network.

Internet

- I will only download items with permission.
- I must close any website that aren't appropriate and tell an adult.
- I will not attempt to access any inappropriate social network sites or chatrooms.
- We only use websites that an adult has chosen or knows about.

Images

- I will only take, store and use images of people for an agreed project or purpose that I have permission for.

Behaviour

- I will only communicate with others online sensibly.
- We can write polite and friendly emails and not create anything to upset others.
- I will make sure that any online or offline activity will not cause the school/centre, staff and any other user, distress or embarrassment.

Respect

- I know that all use of the network is monitored.
- I will treat other people and ICT equipment with care and respect.
- It is my responsibility to respect and follow all of the above conditions which will help to keep me and other's safe while using ICT