IVANHOE SCHOOL

Staff ICT Acceptable Use Policy

Documentation Information			
Reviewed by:	Ivanhoe School Personnel Committee		
Last Reviewed:	23 March 2023	**Next Review:**	March 2025
Review Cycle:	2 Yearly	Ratified by Governors	

Guidance for staff on the safe use of technology:

- Social networking : A guide for Teachers and School staff
- Cyberbullying : Advice for head teachers and school staff
- Email communication : A guide for Teachers and School staff

Ivanhoe School Policy

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

This Acceptable Use Policy is intended to ensure:

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

Ivanhoe School ensure that staff/volunteers/governors will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that all ICT devices are the property of Ivanhoe School, therefore the use of these devices and associated services (i.e. e-mail, internet access) is monitored.
- I understand that the rules set out in this agreement also apply to use of Ivanhoe School ICT systems (e.g. laptops, email, SIMS etc.) out of Academy.
- I understand that the Ivanhoe School ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by Ivanhoe School.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.
- I will not allow anybody to use any of my ICT systems logins – unless required by the ICT Department for technical purposes (e.g. configuring/repairing ICT equipment).
- I understand that my internet access is a filtered connection and no attempt will be made to circumnavigate this.

I will be professional in my communications and actions when using Ivanhoe School ICT systems:

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

General Data Protection Regulation (GDPR)

- I will not remove or copy sensitive or personal data from the school network unless the device is encrypted and stored securely
- I will ensure that any sensitive or personal data will only be printed if there is a valid reason
- Wherever possible, staff should use college software and equipment to access and store information/data. Staff should not export any sensitive, personal or confidential data from the college network and store on personal devices
- Staff should ensure that all sensitive or personal data is kept private and confidential, except when required by law to disclose such information to the appropriate authority.
- Any e-mails sent containing sensitive or personal information, within the body of the e-mail or as an attachment, should be encrypted before sending.

- Staff should ensure that the usage of any online/cloud systems or services has been approved. Explicit consent may be required from the parent and/or student before information can be shared with these services.

- Staff have a responsibility to ensure that any data breaches are reported to the Data Protection Officer immediately. If required, these breaches have to be reported to the Information Commissioners Office within 72 hours of the breach

Ivanhoe School has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy:

- When I use my personal hand held/external devices (laptops/mobile phones/USB devices etc.) in Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will ensure I follow the guidelines provided when using encrypted ICT devices (i.e. USB access keys will not be stored with laptops)

- I will not (unless I have permission) attempt to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in Academy policies.

- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.

- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Ivanhoe School policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

When working from home:

- I will ensure that all communications with parents/guardians/students are carried out with Academy approved systems, and I will follow all standards as if I were within the Academy however in some instances it may be required to use personal equipment. When doing this I will seek approval from the College and I will use functions to safeguard myself e.g. ensure "Caller Withheld" is enabled on my device to prevent parents/guardians/pupils having visibility of my personal contact details
- I will ensure that my device backgrounds/desktops contain images that are suitable should I participate in any screen sharing as part of video conferencing facilities
- I will ensure that any files/emails/document file names are not visible, and no sensitive information is visible should I take part in any screen sharing facilities
- I will ensure that I comply with all GDPR/Data Protection policies and procedures
- I will ensure that I follow the same Academy dress code for video conferences as if I were physically within the Academy building

I understand that I am responsible for my actions in and out of Ivanhoe School:

- I understand that this Acceptable Use Policy applies not only to my work and use of Ivanhoe School ICT equipment within Academy, but also applies to my use of Ivanhoe School ICT systems and equipment out of Academy and my use of personal equipment in Academy or in situations related to my employment by Ivanhoe School.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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

Full Name	
Signed	
Date	
Job Title	

Glossary

Computer Misuse Act

The Computer Misuse Act makes it an offence for anyone to have:-

- Unauthorised access to computer material e.g. if you find or guess another user's password and use it.
- Unauthorised access to deliberately commit an unlawful act e.g. if you guess another user's
  password and access their learning account without permission
- Unauthorised changes to computer material e.g. if you change the desk-top set up on your computer or introduce a virus deliberately to the school's network system.

Data Protection Act 1998

The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school.

The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act not only applies to paper files it also applies to electronic files.

The Principles of the Act state that data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than necessary
- Processed in accordance with data subject's rights
- Secure
- Not transferred to other countries without adequate protection

RIPA – Regulation of Investigatory Powers Act 2002

If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:

- the interception of communications
- the acquisition and disclosure of data relating to communications
- the carrying out of surveillance
- the use of covert human intelligence sources
- access to electronic data protected by encryption or passwords

If a request for authorised access is made to the school, we will provide the appropriate access to your ICT records and files.

Social Networking:

A guide for Teachers and School staff

KEY QUESTIONS

Many Teachers and other staff use social networking services (SNS), such as facebook and Twitter, in order to stay in touch with friends and family. This guide is designed to support your personal use of these services, keeping you, your students, and your job safe.

1: Can I be friends with my pupils on social networking services?

A recent TES survey found that a small percentage (9%) of teachers were friends with their pupils on SNS.[1] It is not a good idea to accept friend requests on your personal accounts[2] or to accept requests to follow you from pupils, recent pupils or even parents at your school. (On most services, the sender won't be notified if you select ignore/not now or delete for such requests, nor, if you had already accepted such a request, will they be notified if you remove them from your friends list or followers). By accepting such requests, you could be making yourself vulnerable by sharing personal information or by having access to personal information about your pupils. You may be potentially leaving yourself open to allegations of inappropriate contact or conduct or even find yourself exposed to unwanted contact. Your school may provide guidance regarding this in their E-safety or Acceptable Use Policy (AUP) and there is clear guidance supported by the Teaching Unions to say that friending pupils is not appropriate[3]. Some educators and schools do use Facebook or other SNS to connect and communicate with pupils, parents, and governors, but they do so using professional or organisational accounts or pages, with prior approval from their Senior Leadership Team (SLT) and recognising that Facebook and many SNS do have a minimum age requirement of 13.

2: Which privacy settings do I need as a teacher if I am using social networking services?

The answer will depend on what you have on your profile, and what you tweet or post. It is important that when using SNS you are in control of who can see your account details and content including photos and albums, posts, status updates and any personal information. On Twitter, you can set your account to private by selecting 'Protect my tweets' so you can then accept (or decline) requests to follow you. In the case of Facebook, choosing a basic 'Friends' setting for every option would initially achieve this. However, you are able to customise each option further, and can limit the information that certain individuals see. It is a good idea to use the "view as" option, to check and see how your profile appears to strangers, and that the information you want to remain private or 'friends only' is not visible. If you are unsure about how to use the settings available, treat all information that you post as being public and act accordingly.

Think carefully about whom you are friends with, and which friends can access what information. It is a good idea to remove any "friends" or customize the privacy settings for current friends, if access to your personal activity could compromise your position, for example parents with

children at your school. However, whatever setting you use, it's important always to think before you post because 'Friends' settings do not guarantee privacy. Sharing content with others could mean that you lose control of it, if friends pass on your information, for example.

Think carefully about comments you post on friends' walls – if their profile is not set to private your posts will be visible to anyone.

3. What about the use of geo-location services?

Geo-location services are beginning to be used by educators to support teaching and learning. However, there are obvious issues in making sensitive information – where you are at a given time or the places you regularly visit – public. When using location services on SNS, think about making your location visible to only your friends and ensure that you are happy with the friends in your list. The option for being 'checked into' a place by someone else can be disabled in your privacy settings, so you can keep control of your location information.

4. How can I continue to protect my professional reputation?

Your professional reputation is clearly valuable to your current and future career and consequentially managing your online reputation is an essential part of being a teacher. Always think carefully before making any posts, status updates or having discussions regarding the school, its staff, pupils or parents in an online environment – even if your account is private. Comments made public could be taken out of context and could be very damaging. Think about the language you use – abrupt or inappropriate comments, even if they were made in jest, may lead to complaints. Anything that is put online is potentially public and permanent. Posting derogatory comments about pupils, parents or colleagues is never acceptable. Teachers are required to uphold the reputation of the school, to maintain reasonable standards in their own behaviour, and to uphold public trust in their profession. Bringing your school or your profession into disrepute may cost you your job.

Use a strong password, and log out of the SNS after using it. Not logging out means the next user of the computer or other access point can access your SNS account. (Deleting cookies may be necessary if you had selected the 'remember this password' option when you were logging in). If you access social networking via an application on your mobile phone, it is a good idea to set a PIN or passcode for the phone, and to remember to log out of the SNS app after each session, so if you mislay your phone, access to your SNS account is still protected.

Be mindful of how you present yourself when you are choosing a profile image, for example, or even when joining a Group or 'liking' pages – think about what these choices say about you.

Consider making private, or removing, previous online content that might compromise your current position. It is possible to deactivate existing SNS accounts and to permanently delete profiles. It is important to be aware, however, that though such changes will be immediate on the service itself, content which was visible on public search may still be visible on public search

results for a week or two (or even longer) until these changes have been recognised by the search engine.

Searching your name regularly on public search engines can be a useful way to monitor your online content or 'digital identity'. Other tools are also available, for example, utilising privacy settings and removing your profi le page from a search engine result. Your online reputation is important for your current and future employment – it is common for employers to search prospective employees online. One recent survey found that 41% of employers in the UK rejected candidates due to data found online[4].

5. What should I do if other people post inappropriate images of me online? How about if I am the victim of cyberbullying?

If you are unhappy with photos in which you are tagged, untag yourself or alternatively contact the friend and ask them to remove this content. Never be shy about asking others to take down or make private content that identifies you that you are not comfortable with. Be thoughtful about content you post that relates to others, and respond positively to requests to take down or make content private. If you think that the image or video breaks the SNS's terms of use, report it to the SNS who can take content down (look for the Report Abuse options in the service).

If you are the victim of cyberbullying, for example, a pupil makes inappropriate comments or posts images of you or another member of staff, don't retaliate and save/print all available evidence (wall posts, URLs, messages, comments, etc.). Schools have a statutory duty of care for the health, safety and welfare of school staff and should therefore take reasonable steps to support staff experiencing cyberbullying. You should report any incident to a member of SLT, other appropriate points of contact within your school could include your line manager. Staff can seek additional support and advice outside of the school; contact your Union or professional association, the Teacher Support Network or the Professionals Online Safety Helpline.

6. What should I do if I see inappropriate content on social networking sites about my pupils?

If you come across, or are made aware of, inappropriate use of social networking sites by your pupils (including under age use of these services), you should report these to the appropriate person within your school – to the Designated Senior Leader who has responsibility for safeguarding. The school has a range of policies and procedures, including its AUP, which relate to the inappropriate use of SNS by pupils.

7. Can I use sites like Facebook or Twitter in school for educational purposes with my pupils?

Most SNS have an age requirement of thirteen. Social networking services are blocked in many schools. However with careful planning and management, they can be used responsibly by educators to provide valuable opportunities for collaborative learning. There has been work reviewing the potential benefits of using SNS with learners, and SNS use in education5 alongside

other technologies. For example see the Cloudlearn.net project, and 'Using Facebook in the Classroom'[6]. If your school supports the positive use of SNS, always seek clear guidance from a senior member of staff if you wish to use these with your pupils. Always act in accordance with school policy.

Further information

Cyberbullying Guidance – supporting school staff

www.digizen.org/resources/school-staff.aspx

Facebook Safety advice for Educators

www.facebook.com/help/?safety=educators

Young people and social networking sites –

a guide for parents, carers and teachers:

www.childnet.com/downloads/blog_safety.pdf

Using Facebook safely: A guide for professionals

working with young people published by the

Yorkshire and Humber grid for learning:

http://tinyurl.com/4yumvor

1 See http://community.tes.co.uk/forums/t/463065.aspx?s_cid=16

2 See **http://fraser.typepad.com/socialtech/digital_literacy**

3 See p6 of Supporting School Staff: Cyberbullying

4 See www.microsoft.com/presspass/features/2010/jan10/01-26dataprivacyday.mspx

5 See for example, http://www.digizen.org/socialnetworking/benefi ts.aspx, and see for example,

'33 Interesting Ways to Use Twitter in the Classroom'

https://docs.google.com/present/view?id=dhn2vcv5_118cfb8msf8

6 See www.heppell.net/facebook_in_school

www.digizen.org/resources/school-staff.aspx

Department for Education

Cyberbullying: Advice for headteachers and school staff

Who is this advice for?

This is non-statutory advice from the Department for Education for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

Overview

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. It is important that schools take measures to prevent and tackle bullying among pupils. But it is equally important that schools make it clear that bullying of staff, whether by pupils, parents or colleagues, is unacceptable. Evidence indicates that one in five (21%) teachers have reported having derogatory comments posted about them on social media sites from both parents and children.

School leaders, teachers, school staff, parents and pupils all have rights and responsibilities in relation to cyberbullying and should work together to create an environment in which pupils can learn and develop and staff can have fulfilling careers free from harassment and bullying.

Schools can offer support to parents on how to help their children engage safely and responsibly with social media, perhaps through a parents' evening, advice in a school newsletter or signposting to other sources of support and advice. Creating a good school- parent relationship can help create an atmosphere of trust that encourages parents to raise concerns in an appropriate manner. Part of this is making sure that parents and carers are aware and understand how to communicate with the school. Schools should also make clear that it is not acceptable for pupils, parents or colleagues to denigrate and bully school staff via social media in the same way that it is unacceptable to do so face to face.

Schools should encourage all members of the school community including parents to use social media responsibly. Parents have a right to raise concerns about the education of their child, but they should do so in an appropriate manner.

School staff

- All school staff are in a position of trust, and there are expectations that they will act in a professional manner at all times. Here is some key advice for staff which may help protect their online reputation:

- Ensure you understand your school's policies on the use of social media, Childnet's 'Using Technology' guide has more information on what to be aware of.

- Do not leave a computer or any other device logged in when you are away from your desk.

- Enabling a PIN or passcode is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by pupils.

- It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The UK Safer Internet Centres Reputation minisite has more information on this.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Consider your own conduct online; certain behaviour could breach your employment code of conduct.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Do not accept friend requests from pupils past or present. If you feel this is necessary, you should first seek guidance from a senior manager. Be aware that your social media friends may also be friends with pupils and their family members and therefore could read your post if you do not have appropriate privacy settings.
- Do not give out personal contact details – if pupils need to contact you with regard to homework or exams, always use your school's contact details. On school trips, staff should have a school mobile phone rather than having to rely on their own.
- Use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

If you are bullied online

- You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.
- If they refuse, it should be an organisational decision what to do next – either the school or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police. Online harassment is a crime.

Employers have a duty to support staff and no-one should feel victimised in the workplace. Staff should seek support from the senior management team, and their union representative if they are a member. The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff

face, such as protecting professional identity, online harassment, or problems affecting young people; for example, cyberbullying or sexting issues.

The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more.

Schools

Whole-school policies and practices designed to combat bullying, including cyberbullying, should be developed by and for the whole school community. All employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff and supporting them if it happens.

Schools should develop clear guidance to help protect every member of the school community and to ensure that sanctions are appropriate and consistent. This will need to be effectively communicated to and discussed with employees, pupils and parents. Kidscape has also produced best practice advice and guidelines for professionals. The Diana Award also runs a whole school Anti-Bullying Programme, information and good practice can be found at www.antibullyingpro.com.

Reporting

The whole school community should understand reporting routes and responsibilities. Many schools will appoint a designated person to deal with bullying while others will distribute responsibility among a number of staff.

Acceptable use policies

- Every school should have clear and understood policies in place that include the acceptable use of technologies by pupils and staff that address cyberbullying. Agreements on the responsible use of technology should include:

- Rules on the use of school equipment, software and access routes when used on or off the school premises within school hours: for example, internet access, tablets, lap tops and mobile phones.

- Acceptable behaviour for pupils and employees, including behaviour outside school: for example, teachers' and pupils' use of social networking services and other sites, so as not to harm others or bring the school into disrepute.

- School staff should expect the school to react quickly to reported incidents or support the member of staff concerned to do so. It is also important that staff who are harassed in this way receive support and information enabling them to access appropriate personal support. The school should endeavour to approach internet providers or other agencies on their behalf in order to request that the inappropriate material is removed. The internet provider may only accept a request from the victim. However, the school may want to take action if it is on a school website or email address.

- If it is necessary for the person being bullied to contact the service providers directly, the school may provide support. This might apply, for example, in cases of identity theft, impersonation or abuse via a mobile phone service.

Useful resources

The Parent Zone has established a training programme designed to enable schools and professionals working with parents to deliver their own sessions on internet safety. They also provide innovative resources for schools to help and support parents, particularly around e-safety.

Facebook has produced Empowering Educators support sheet specifically for teachers and launched the Bullying Prevention Hub with Yale's Centre for Emotional Intelligence.

Getting offensive content taken down

If online content is offensive or inappropriate, and the person or people responsible are known, you need to ensure they understand why the material is unacceptable or offensive and request they remove it.

Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material, the staff member should use the tools on the social networking site directly to make a report.

Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.

Before you contact a service provider, it is important to be clear about where the content is; for example, by taking a screen shot of the material that includes the web address. If you are requesting they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions. Where the material is suspected of being illegal you should contact the police directly.

Contact details for social networking sites

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools.

Social networking site	Useful links
Ask.fm	• Read Ask.fm's 'terms of service' • Read Ask.fm's safety tips • **Reporting on Ask.fm:** • You do not need to be logged into the site (i.e. a user) to report. • When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post.
BBM	• Read BBM rules and safety
Facebook	• Read Facebook's rules • Report to Facebook • Facebook Safety Centre
Instagram	• Read Instagram's rules • Report to Instagram • Instagram Safety Centre
Kik Messenger	• Read Kik's rules • Report to Kik • Kik Help Centre
Snapchat	• Read Snapchat rules • Report to Snapchat • Read Snapchat's safety tips for parents
Tumblr	• Read Tumblr's rules • Report to Tumblr by email • If you email Tumblr take a screen shot as evidence and attach it to your email
Twitter	• Read Twitter's rules • Report to Twitter
Vine	• Read Vine's rules • Contacting Vine and reporting
YouTube	• Read YouTube's rules • Report to YouTube • YouTube Safety Centre

Mobile phones

All UK mobile phone providers have malicious or nuisance call, text or picture message centres set up and have procedures in place to deal with such instances. If you are being bullied they will help you to change your number if necessary. If you want to prosecute the perpetrator contact the police. The mobile provider will work closely with the police and can usually trace malicious calls for them.

Service providers: Service provider	**From your mobile**	**Pay as you go**	**Pay monthly contracts**
O2	4445 or 202	08705 678 678	0870 241 0202
VodaFone	191	03333 040 191	03333 048 069
3	333	08433 733 333	08433 733 333
EE	150	0800 956 6000	0800 956 6000
Orange	150	07973 100 450	07973 100 150
T-Mobile	150	07953 966 150	07953 966 150
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751

Reference: DFE-00652-2014

Email Communication:

A guide for Teachers and School staff

The following points support best practice in the use of Ivanhoe's email system. Users are strongly encouraged to adopt these points wherever possible.

Respond promptly

- If a full answer is not possible within this timescale, send an acknowledgement email with details of when a full response will be sent.
- The full response must be within ten working days
- You should set up your out of office reply if you are unable to access your email account for more than a day and include an alternative contact in the message
- Staff should also aim to respond to internal emails within the same timeframes as above

Write clearly and concisely

- Your message should be easy to read and understood, using plain English rather than jargon – see www.plainenglish.co.uk for more information
- Adapt the tone according to the situation. For example, a response to a formal external email should be replied to formally, but an internal email to a colleague can be more informal
- Don't go into more detail than is required. A concise email is quicker to deal with by the recipient than a rambling one
- Only attach documents when necessary and refer to them in the email.
- Name attachments properly so the recipient knows what is being attached
- Make it clear what action, if any, is expected in response to your email
- Read all messages through and spell check them before you press 'send'

Manage email effectively

- Email attachments should be detached and stored on local shared network drives or deleted within twelve months of receipt, rather than stored within your email account
- If storing emails for a short period, make use of the ability to file emails within folders, rather than keeping all emails in your inbox
- Email attachments like Word documents and PDFs take up large amounts of storage space. They should be removed from emails you wish to store and saved on local network drives if required
- Your emails should consume no more than 100MB storage space at any given time. If you go above this, an automatic warning will be sent to you
- Try to keep to a maximum of 100 messages in your inbox and 1000 in total throughout your email folders. Weed out your 'sent items' folder regularly. This should help you manage your email and prioritise your work effectively

Be aware of Freedom of Information (FOI) and data protection legislation

- All emails, regardless of length, are public records. There is no distinction between information contained in an email and any other document
- You need therefore to be aware that what you write in an email could become disclosable and therefore available to the public

- Keep personal information about individuals to a minimum and dispose of that information as soon as the need to use that information has passed
- FUS may where required use data protection legislation to check users email accounts in their absence. However, if an email is marked 'personal', this will be respected unless there is a business case to do otherwise
- Under FOI, the public have a right to request information held by the Council, unless it is exempt. It is therefore important that you compose emails with this in mind and that any important emails are stored on shared servers so they can easily be accessed by colleagues if required
- Check if unsure about any of the above points

Be aware that emails are not secure

- Whilst internal emails sent within the EMBC network are secure, external emails are not a very secure means of transferring sensitive or confidential information
- This is because they are relatively easy to intercept by hackers. You should therefore think very carefully before sending external emails that contain highly personal or confidential information.

When not to send email

- If using the telephone or meeting face-to-face would be more effective
- Think carefully about whom you send messages to. Do they really need to be sent or copied into the message?
- When the information is or should be available on the School network
- To numerous people, even if you are just copying them in – reading unnecessary emails wastes time and overflowing inboxes can cause stress. Only include people if they really need to see the message
- Do not attach large documents or use formats that recipients may not have.
- In haste, particularly if you are angry - wait to calm down so your response is more measured

And lastly

- Do not open attachments from people you don't know. They can be used to spread viruses
- Always use the default email font
- Always use the 'subject' field with a clear indication of what the message is about. This helps recipients prioritise emails and find the one they need amongst all the others
- Do not store documents attached to emails in your email folders. This creates individual islands of data, which are hugely inefficient in terms of IT storage and can cause version control issues. Save documents on the local network drives instead
- If replying to an email, include enough, but not necessarily all, of the original message in your response to keep the thread of the conversation clear
- Apply the same professionalism you do to other forms of communication such as telephone and letter
- With external emails, ensure you include a signature that includes a minimum of your contact name, title and telephone number
- Do not print out all emails you receive. This wastes paper, toner and time and is usually unnecessary as most emails can be dealt with on screen

- That using 'return receipt' increases traffic unnecessarily, please only use when essential and be aware that it often won't work if sending external emails
- If you receive an email that was sent to you in error, stop reading it as soon as this becomes obvious. Then return it to the sender and delete it
- Be on your guard for scam emails, asking you to enter personal information, for example your bank security details
- Also be wary of alarmist emails that are often hoaxes