The Fraserburgh Way

E-Safety

Edition 2

Dec 2020

The Fraserburgh Way

Our Values

Aspiration
Community
Integrity
Kindness
Trust

Our Routines

Hands Up For Silence
Meet & Greet
End & Send
Walk & Talk

Our Repair

What happened?
How were you feeling?
Who was affected?
How might they have been feeling?
What needs to happen?

Our Recognition

Praise in Public, Reprimand in Private
Recognition boards
Postcards
Lighthouse Awards

Our Phrases

" Right Time, Right Place, Right tone, Thank you."
"I hear what you are saying now I need you to .."
"Phones away for learning, Thank You."
"Round in 5 for learning, Thank You."

Our Response

"I hear what you are saying. The rule was about being R/R/S. I have seen you doing this really well before. I need you to be more R/R/S. Thanks for listening."

Contents

Introduction	4
Development, Monitoring & Review of this Policy	5
Roles and Responsibilities	6-8
Filtering	9-10
Personal devices	11
User Behaviour	11-12
Responding to Incidents of Misuse	13
Appendices	14-17

Introduction

Technology is seen as a **fundamental resource** to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. In order to build the **skills** to better prepare our young people for **life, learning and work**, it is essential that we **incorporate the use of technology into our curriculum**. At Fraserburgh Academy, we are committed to ensuring that **all our staff and learners** are able to:

- Use digital platforms to enable anytime-anywhere learning.
- Use a range of digital tools to enhance lessons.
- Use digital technologies outside of school safely.

- Adapt their skills as technology evolves.

This policy applies to all **stakeholders** of Fraserburgh Academy (staff, learners, volunteers, parents/carers, visitors, community users) who have **access to and are users** of Fraserburgh Academy digital technology systems, both **in and out** of the school.

It is important to emphasise that behavioural/safeguarding issues are not digital technology issues, simply that the technology provides additional means for behavioural/safeguarding issues to develop.

The school will deal with behavioural/safeguarding issues in accordance with this policy and our associated behaviour, anti-bullying and safeguarding policies. Where known incidents of inappropriate or unsafe behaviour occur, the school will share information with parents/carers and other partners as appropriate.

GO TO
BETTER RELATIONSHIPS, BETTER LEARNING, BETTER BEHAVIOUR

GO TO
ANTI-BULLYING POLICY

GO TO
SCHOOL HANDBOOK FOR BEHAVIOUR & ETHOS

Development, Monitoring & Review of this Policy

This online safety policy has been developed by the Fraserburgh Academy E-Safety Group made up of:

SLT members	Ed Walton (DHT Digital Learning) & Irene Sharp (HT)
Child Protection Coordinator	Pamela Whyte (DHT Support)
Online Safety Officer	Chris Goan (PT Digital Learning)
Teaching staff member	Faculty Digital Leaders
Support staff member	Lesley Muir (Cluster Busines Manager)
Parent / Guardian	Pearl Morrison
ICT Technical Support staff	Jason Monger/ Fergus Pirie Aberdeenshire ICT
Children/young people representation – for advice and feedback	Ryan Broadly – Learner Engagement

Consultation with the whole school community has taken place through digital questionnaires.

Schedule for Development, Monitoring & Review

This online safety policy was approved by ECS Technology Development Manager (Aberdeenshire Council) on:	18th Dec 2020 (Proposed)
The implementation of this online safety policy will be monitored by the:	E Safety Group
Monitoring will take place at regular intervals:	Yearly
The Authority will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	At least once a year
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Feb 17th 2021 – End of first 6 weeks of Wifi Switch on Staff, Student and Parent Survey
Should serious online safety incidents take place, the following external persons/agencies should be informed:	SLT informed before: Aberdeenshire Council (QIO) **Craig Sim** ECS Technology Development Manager **Graeme Slapp** Police Social Work Other relevant agencies

The school will monitor the impact of the policy using:

- Logs of reported incidents – **SEEMIS Pastoral Notes & DHT Digital log.**
- Internal investigating/reporting of inappropriate internet activity (including sites visited) – **DHT Digital log.**
- Raise filtering concerns with Aberdeenshire ICT - **DHT Digital**
- Internal investigating/reporting of inappropriate activity on network **SEEMIS Pastoral Notes & DHT Digital log**
- Surveys of learners & Parents.
- Staff Feedback via policy monitoring calendar

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Fraserburgh Academy.

Aberdeenshire Council

The school will work very closely in partnership with officers from Aberdeenshire Council to ensure that the schools' policies and procedures are in line with local and national advice and inter-agency approaches to the care and wellbeing of children and young people.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the DHTs with support of Online Safety Officer.
- The Headteacher, Senior Leadership Team and QIO should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer.
- The SLT/PTG records incidents of online bullying through the school's SEEMiS recording system in line with local procedures.
- The DHT(Digital) maintains a log of incidents to inform future online safety developments.
- The DHT(Digital) meets with Learning Through Technologies team to discuss current issues.

Online Safety Officer

- Chairs the E - Safety and Digital Leaders Team.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff on designated GLOW Team Help and Update Channel https://teams.microsoft.com/l/channel/19%3ae805d567a89d49ee8e9168e92ca83b47%40thread.tacv2/ICT%2520Updates%2520and%2520Help?groupId=a4eee243-4ff9-46c4-96f2-2aff6ca61257&tenantId=ccd32ca3-16ce-428f-9541-372d6b051929
- Liaises with SLT/Aberdeenshire ICT/ECS Technology Development Manager, when appropriate.
- Liaises with school technical staff.
- Receives reports of online safety incidents (serious incident form/GIRFEC/Child Protection) and creates a log of incidents to inform future online safety developments. This is passed to DHT Digital.
- Meets twice a term with DHT Digital to discuss current issues, review incident logs and report filtering issues.
- Attends relevant meetings of SLT/Authority.

Aberdeenshire Council ICT

Aberdeenshire Council ICT is responsible for ensuring:

- That the school technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation and action

Technical – *infrastructure, equipment, filtering & monitoring*

Aberdeenshire Council will be responsible for ensuring that the school infrastructure and network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority Online safety Policy and guidance).
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems.
- Aberdeenshire ICT are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- School systems are in place for users to report any online safety incident to the DHT Digital.
- GDPR training is made available for staff to ensure protected data is not put at risk.

Teaching and Support Staff

Are responsible for ensuring that:

- They have read, understood and signed the staff acceptable use policy (AUP).
- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They report any suspected misuse or problem to the DHT Digital for investigation.
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in aspects of the curriculum (PSE, BECS & APEX) and other activities.
- Pupils understand and follow the Online Safety Policy and acceptable use policies as per AUP.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed as per discretion of teacher) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

DHT Pastoral Support

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Grooming.
- Online bullying.

E - Safety Group

The E - Safety Group provides a consultative group that has wide representation from Fraserburgh Academy community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy.

Members of the E - Safety Group will assist the DHT Digital with:

- The Review & Monitoring of the school online safety policy.
- Consulting stakeholders – including parents/carers and the pupils about digital provision.

Learners

- **Are responsible for using Fraserburgh Academy's digital technology systems in accordance with the pupil acceptable use policy.**
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, PTG in first instance.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that Fraserburgh Academy's online safety policy covers their actions out of school, if related to their membership of the school.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' information evenings, newsletters, letters, website, social media and information about national/local online safety documentation. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and on-line pupil records

Community Users

Community Users who access Fraserburgh Academy systems or programmes as part of the wider school provision will be expected to sign a Community User AUP before being provided with access to school systems. Visitors to the school will have access to our wifi and so will be given a statement of fair use at the point of signing into the school.

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by ICT. They will manage the school filtering, in line with this policy and will keep records of changes.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service will be logged in change control logs.

All users have a responsibility to report immediately to ICT any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering systems in place to prevent access to such materials. Any learners who are found to be attempting this will be dealt with via the behaviour and ethos policy.

Policy Statements

Internet access is filtered for all users. Illegal content is filtered by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the council's network infrastructure, filtering will be applied that is consistent with school practice.

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or other nominated senior leader.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- Any filtering issues should be reported immediately to DHT Digital.
- Requests from staff for sites to be removed from the filtered list will be considered by ICT, Liaising with the ECS Technology Development Manager where appropriate.
- All requests for changes to the filtered list must come via the DHT Digital.

Education, Training & Awareness

Young people will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- The Acceptable Use Agreement.
- Induction training.
- Staff meetings, briefings, Inset.

Parents/carers will be informed of the school's filtering policy through the Acceptable Use Policy and through e-safety awareness sessions and the online portal.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered should report this in the first instance to the DHT Digital. Similarly requests for Filter changes should be sent via the DHT Digital, with a clear rationale communicated.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement.

Audit

Logs of filtering change controls will be made available to the ECS Technology Development Manager on request.

Mobile Devices

Learners will be able to use mobile devices in school in order to assist in their learning. Mobile devices may be school provided or privately-owned: smartphones, tablets, notebooks, laptops or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which will include the school's learning platforms of Microsoft Teams and Google Classroom and other GLOW services such as email and data storage.

The absolute key to considering the use of mobile devices is that young people, staff and the wider school community understand that the primary purpose of having their device at school is educational and that this is irrespective of whether the device is school provided or personally owned. The mobile policy will sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, policies around theft or malicious damage and the behaviour policy.

Personal devices

When personal devices are permitted:

- All personal devices are restricted through filtered network access.
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user as does the liability for any loss or damage resulting from the use of the device in the school.
- Beyond Glow, staff personal devices should not be used to contact young people or their families, nor should they be used to permanently store images of young peoples.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the school or on activities organised or undertaken by the school.
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable, have a protective case and are always secured with a random passcode or pin.
- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Personal devices should be charged before being brought to the school as the charging of personal devices may not be available during the school day.

User Behaviour

Users are expected to act responsibly, safely and respectfully in line with current acceptable use policies, in addition;

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the behaviour policy.
- Guidance is made available by the school to users concerning where and when mobile devices may be used.
- Devices may not be used in tests or exams.
- Users are responsible for keeping their device up to date through software, security and app updates. The device has to be virus protected and should not be capable of passing on infections to the network.
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school.
- Devices must be in silent mode on the school site and on school buses.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Children / young people must only photograph people with their permission and must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately.
- Devices may be used in lessons in accordance with teacher direction.

User Actions

Some internet activity, e.g. accessing child abuse images or distributing racist material is illegal and is banned from school and all other technical systems. Other activities, e.g. online bullying/hate crime is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but are inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in, or out of, school when using school equipment or systems. The school policy restricts usage as follows:

	User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography					X
	Promotion of any kind of discrimination					X
	Threatening behaviour, including promotion of physical violence or mental harm				X	X
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)			X			
On-line gambling					X(S)	X(P)
On-line shopping / commerce					X	
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. YouTube			X			

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a ready, respectful and safe approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, report to a Duty Manager who take immediate action via Year Head or the Headteacher, including Parental contact, and possible Police involvement. The DM will also make contact with the Child Protection Officer as appropriate.

Inappropriate Incidents

There may be times when infringements of the policy take place, through careless, irresponsible or, on occasion, through deliberate misuse.

Procedure:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the investigation using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure
- Record the sites and content visited (to provide further protection):
    - the URL of any site containing the alleged misuse and describe the nature of the content causing concern.
    - store screenshots of the content on the machine being used for investigation.
- Once this has been completed and fully investigated the two senior staff members will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures (**staff**).
    - School sanctions and parental involvement (**student**).
    - Involvement by local authority or national/local organisation (as relevant) (**staff/student**)
    - Police involvement and/or action. (**staff/student**)
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to DHT Child Protection and the police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour.
    - the sending of obscene materials to a child.
    - adult material which potentially breaches the Obscene Publications Act 1964.
    - criminally racist material.
    - promotion of terrorism or extremism.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by DHT Digital for evidence and reference purposes.

School Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been resolved through engagement with learners, parents, staff and others involved, plus any necessary sanctions have been issued. It is intended that incidents of misuse will be resolved through the school's positive ethos policy. Our aim will be to bring learners back to being Ready Respectful and Safe while using their technology.

BYOD Staff Update

Appendix 1

You and your devices

Full Aberdeenshire Code of Practice on BYOD can be found here.

The usual Acceptable Use Policy for council machines applies to your own device when you are using it in school. Be extra vigilant about blurring the lines with photos, moving data and so on when using your device.

Supporting Learners with BYOD

Named roles: **DHT Digital - Ed Walton, CPO - Pam Whyte**

1. What to be vigilant for with **Learner Safety**:

Insecure login codes or passwords
Refer to PTG (OTB)

Arranging to meet an online contact in person
Refer to DM/CPO -Skype

Stranger danger
Refer to DM/CPO - Skype

Logging in as other people
Refer to Year Head - email

Disclosure online of personal data
Refer to DM/CPO - Skype

2. What to be vigilant for with **Inappropriate Use**:

Inappropriate content (Accidental)
Refer to DHT Digital for filtering review - email

Inappropriate content (intentional)
Refer to PTF for minor (OTB)
Call a DM for a serious breach - Skype

Non-educational use of tech in class
Refer to PTF (OTB)

Unfair upload/download size
Refer to DHT Digital - email

File sharing, video broadcasting outside of teacher permission
Refer to PTF or PTG if at social time (OTB)

Gambling, shopping
Refer to PTG (OTB)

3. What to be vigilant for with **Disrespectful Use**:

Files belonging to other people: copying, deleting, altering

Refer to PTF if serious breach (OTB)

Disrespectful Communication: aggressive, inappropriate, anti-social

Refer to PTF/PTG as appropriate (OTB)
Call a DM for a serious breach

Bullying

Refer to PTG (OTB)

Photos without consent

Accidental – ensure deleted
Intentional or refusal - PTF/DM

Disrespectful behaviour online to do with the school, even if undertaken away from school

Refer to DHT Digital - email

Distribution of photos/data

Refer to PTG (OTB)
Sexualised data DM/CPO - Skype

4. What to be vigilant for with **Right Time, Right Place**:

Using Tech in class without permission

Refer to PTF if persistent (OTB)

Device not in silent mode

Refer to PTF if persistent (OTB)

Social Media use in class time (in classroom or in corridor)

Refer to PTF if persistent (OTB)

Attempting to bypass filter system

Refer to DHT Digital - email

Appendix 2

Record of reviewing devices/internet sites
(responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Asset num and location of computer used for review (for web sites)

Web site(s) address/device	Reason for concern

Conclusion and action proposed or taken

Appendix 3

Reporting Log Template **Fraserburgh Academy**						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

FRASERBURGH

DIGITAL EXPECTATIONS

SAFE

- Keep your login details safe
- No one else logs in as you
- Never meet someone in person, after only knowing them online - tell someone if you're asked to do this
- Be careful with photos from your phone - they will have data on where and when you took it!
- Never share your personal data
- Stranger danger

APPROPRIATE

- Don't do file sharing or video broadcasting unless you have Teacher say-so
- Be fair with other users - big uploads and downloads will slow everyone down!
- Be careful what you search for, accidents can happen
- In class, only use your device for learning
- Keep searches appropriate for a school setting

RIGHT TIME RIGHT PLACE

- In Class, always ask for permission to use your device
- Keep your device on silent mode, until invited to share sound.
- In Class, do not use social media, **focus on learning**!
- The filter is there for a reason, do not attempt to bypass it.

RESPECTFUL

- Respect other people's files: no copying, deleting, altering
- Respect others online: no aggressive, anti-social or offensive messages
- Don't be a cyber bully
- Don't share or post photos or data that belong to someone else
- If referring to the school online, be respectful
- Check for consent before taking photos

FRASERBURGH ACADEMY

TOGETHER CREATING POSITIVE FUTURES

Monitoring & Review

Date	Changes made	Pages	Changed by
Dec 2020	Wholesale style changes Major rework of all sections.	Throughout	EW DHT Digital in response to Pupil Questionnaire, Pupil and Staff engagement